

Einsatzmöglichkeiten der Blockchain-Technologie in der Logistik

Torben Steffen
(Matrikelnummer: 70381843)

Eingereichte Abschlussarbeit
zur Erlangung des Grades

Bachelor

Im Studiengang

Transport- und Logistikmanagement
an der

Karl-Scharfenberg-Fakultät

der Ostfalia Hochschule für angewandte Wissenschaften

Erster Prüfer: Prof. Dr. Frank Ordemann

Eingereicht am: 02.10.2018

Zweiter Prüfer: B.Sc. Marius Trost

Inhaltsverzeichnis

Abbildungsverzeichnis	iii
Tabellenverzeichnis	iii
Abkürzungsverzeichnis	iii
1 Einleitung	1
1.1 Problemstellung	1
1.2 Ziel der Arbeit	2
1.3 Aufbau der Arbeit	3
2 Grundlagen der Blockchain	4
2.1 Die Geschichte der Blockchain	4
2.2 Die Funktionsweise der Blockchain – Technologie	5
2.2.1 Grundlagen	6
2.2.2 Hashing	11
2.2.3 Konsens-Mechanismen	14
2.2.4 Smart Contracts	18
2.2.5 Öffentliche und private Blockchains	21
2.3 Schlüsselherausforderungen	21
3 Anwendungsbereich Logistik	26
3.1 Erhöhung der Transparenz entlang der Supply Chain	26
3.2 Automatisierung von Zahlungsprozessen	27
3.3 Praxisbeispiele	28
3.3.1 IBM & Maersk	28
3.3.2 GS1	34
4 Schritte zur Blockchain – Implementierung	39
5 Fazit und Ausblick	44
Quellenverzeichnis	46
Eidesstattliche Erklärung	50

Abbildungsverzeichnis

Abbildung 1 Dezentrales (links) und zentrales (rechts) Netzwerk im Vergleich ____	7
Abbildung 2 Veranschaulichung von asymmetrischer Kryptographie _____	8
Abbildung 3 Erstellung und Überprüfung einer digitalen Signatur mithilfe asymmetrischer Verschlüsselung _____	9
Abbildung 4: Vereinfachte Darstellung der Verkettung der einzelnen Blockchain- Blöcke _____	12
Abbildung 5 Transaktionen pro Sekunde von Bitcoin, Ethereum und VISA ____	23
Abbildung 6 Screenshot der Smartphone-App _____	37
Abbildung 7 Phasen des Pilotprojektes zur Digitalisierung des Palettenscheins	42

Tabellenverzeichnis

Tabelle 1 Unterschiede der Blockchains von Bitcoin, Ethereum und Hyperledger Fabric _____	31
--	----

Abkürzungsverzeichnis

ASIC	application specific integrated circuit
ETC	Ethereum Classic
ETH	Ethereum
GLN	Globale Lokationsnummer
PBFT	Practical Byzantine Fault Tolerance
RFID	radio-frequency identification

1 Einleitung

In der Einleitung gebe ich eine Übersicht über die Problemstellung, welche diese Arbeit behandelt, welches Ziel sie verfolgt und welchen Aufbau ich gewählt habe um dieses Ziel zu erreichen.

1.1 Problemstellung

Dass Peer-to-Peer-Systeme (Netzwerke gleichberechtigter Teilnehmer) einen enormen Einfluss auf etablierte Branchen haben können, zeigte sich mit der digitalen Tauschbörse *Napster*. Mit der Entwicklung des mp3-Dateiformats lag Musik in immaterieller Form vor und konnte über die Tauschbörse direkt mit anderen Nutzern auf der ganzen Welt ausgetauscht werden. Die etablierten Plattenlabels wurden einfach durch das Netzwerk ersetzt (dieser Prozess wird auch Disintermediation genannt) und erlitten in der Folge enorme finanzielle Verluste. Durch die geringen Kosten für das Kopieren und Übertragen der digitalen Daten war diese Branche besonders anfällig für diese Veränderung. Dieser Wandel ist theoretisch auf jede vergleichbare Branche übertragbar und kann nach den Musikverlagen auch andere, vorrangig als Vermittler auftretende Dienstleister betreffen.

Besonders hervorzuheben ist hier die Finanzindustrie. Ein Großteil ihrer Tätigkeit ist die Zuordnung von Vermögen auf die Konten der einzelnen Teilnehmer und Transaktionen zwischen diesen.¹ Generell vertrauen wir den Banken unser Geld an. Wir vertrauen diesen zentralen Institutionen, dass sie unsere Vermögen vor unberechtigten Zugriffen schützen und alle getätigten Buchungen im Bankensystem korrekt und autorisiert sind. Einem Peer-to-Peer-Netzwerk, in dem theoretisch jeder Mensch Mitglied werden kann, bringen wir dieses Vertrauen zunächst einmal nicht entgegen. Wir wissen nicht, wie vertrauenswürdig und zuverlässig die anderen Teilnehmer sind. Einzelne Nutzer könnten zweifelhafte Absichten haben und versuchen den Betrieb des Netzwerkes zu manipulieren oder zu stören. Ebenso könnte deren private Hardware, auf der dieses Netzwerk aufgebaut ist, fehlerhafte Daten erzeugen oder sogar ausfallen. An dieser Stelle kommt die Blockchain ins

¹ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.40ff

Spiel. Sie soll Vertrauen schaffen, Integrität im Netzwerk erreichen und diese dauerhaft erhalten.²

Dass die Blockchain-Technologie funktioniert, zeigt sich beim täglichen Einsatz für diverse Kryptowährungen, wie zum Beispiel Bitcoin, um die in letzter Zeit ein regelrechter Hype entstanden ist. Um Überweisungen abseits von Banken zu tätigen, kann diese Technik bereits eingesetzt werden. Aber bieten sich noch andere, speziellere Einsatzmöglichkeiten an als nur eine weitere Bezahlmethode? Immerhin sieht das Weltwirtschaftsforum „die Blockchain-Technologie als einen der sechs Megatrends der nächsten Jahre.“³ „Die Grundidee der Blockchain – eine transparente dezentrale Datenbank, die weder gehackt noch manipuliert werden kann – ist auf alle möglichen Bereiche übertragbar.“⁴ So soll die Blockchain nicht nur für Finanzgeschäfte, sondern auch als Grundlage für beispielsweise elektronische Wahlen oder Crowdfunding-Aktionen genutzt werden.⁵ Auch in der Logistik soll es großes Einsatzpotential geben. Konkret sollen mithilfe der Blockchain unter anderem digitale Dokumente erstellt, Transaktionen automatisiert und Transportwege zurückverfolgt werden.⁶

1.2 Ziel der Arbeit

Das Hauptziel dieser Arbeit ist es, dem Leser mögliche Einsatzszenarien der Blockchain-Technologie im Bereich der Logistik aufzuzeigen, da sie hier bisweilen selten eingesetzt wird. Bereits laufende und aktuelle Feldversuche verschiedener Unternehmen werden dabei näher beleuchtet. Da die Technologie noch neu und vielen Unternehmen noch nicht geläufig ist, werde ich im Folgenden zunächst die grundsätzliche Funktionsweise der Blockchain erläutern. Der Fokus liegt dabei auf dem Verstehen des Ablaufs: Was passiert, welche Prozesse laufen ab und welche Möglichkeiten und Einschränkungen ergeben sich. Die genauen technischen Prozesse im Hintergrund sind nicht Teil dieser Arbeit. Daher werden zu detaillierte

² Drescher, D., Blockchain Grundlagen, Frechen 2017, S.50f

³ Sixt, E., Bitcoins und andere dezentrale Transaktionssysteme, Wiesbaden (2017), S.177

⁴ Specht, P., Die 50 wichtigsten Themen der Digitalisierung, S.219

⁵ Ebd., S.220

⁶ Radermacher, M., Internet of Things und Blockchain in der Logistik, in: www.mm-logistik.vogel.de (abgerufen am 24.09.2018)

und technische Abläufe ebenso wie kryptographische und mathematische Formeln ausgespart.

1.3 Aufbau der Arbeit

Im Anschluss an diese Einleitung gehe ich zunächst auf die Geschichte der Blockchain-Technologie ein. Ebenso werde ich die Funktionsweise wie technische Voraussetzungen, Abläufe und Möglichkeiten dieser Technologie erklären und auch die Herausforderungen, vor die uns diese Technik stellt, werde ich erläutern. Anschließend zeige ich, in welchen Bereichen diese bisher hauptsächlich in der Finanzwelt und dort insbesondere im Bereich der Kryptowährungen anzutreffende Technologie in der Logistik eingesetzt werden kann. Neben allgemeinen Möglichkeiten werde ich auch Praxisbeispiele vorstellen, in denen Unternehmen die Blockchain-Technologie bereits unter alltäglichen Bedingungen im Tagesgeschäft einsetzen. Mit den nötigen Schritten zur allgemeinen Implementierung, um diese Technologie standardmäßig zu nutzen und einem abschließenden Fazit endet schließlich meine Arbeit.

2 Grundlagen der Blockchain

Dieses Kapitel vermittelt grundsätzliches, allgemeines Wissen zum Thema Blockchain und soll den Leser mit diesem vertraut machen. Nach einem Abschnitt zur Entstehungsgeschichte folgen die Grundlagen und einzelne Funktionen.

2.1 Die Geschichte der Blockchain

Bereits in den Neunzigern gab es erste Ideen und Entwicklungen zum dezentralen und verschlüsselten Datenaustausch. Mithilfe dieser Konzepte entstand der heute sehr bekannte Bitcoin und die dafür genutzte Blockchain.⁷ Unter dem Pseudonym Satoshi Nakamoto wurde am 31. Oktober 2008 das neue elektronische Zahlungssystem per E-Mail-Verteiler verbreitet und vorgestellt. In diesem sollen Transaktionen nicht mehr wie bisher über eine Bank als vertrauenswürdige Instanz abgewickelt werden. Nach Nakamotos Auffassung sind Banken keine solchen vertrauenswürdigen Institutionen, was wohl auch seine Motivation für die Entwicklung von Bitcoin erklärt. Stattdessen wird in seinem System ein Peer-to-Peer-Netzwerk genutzt, welches ohne vermittelnde Instanz zwischen den Teilnehmern auskommt. Alle Transaktionen zwischen den Teilnehmern werden auf der dezentral im Netzwerk gespeicherten Blockchain gesichert, anstatt auf einem zentralen Server. Nur wenige Tage nach seiner E-Mail erschuf Satoshi Nakamoto den ersten Bitcoin und startete damit die Bitcoin-Blockchain. In der Folge bildete sich eine rasch wachsende Community. Zur ersten wirklichen Bezahlung mit Bitcoins kam es jedoch erst am 22. Mai 2010. Der Amerikaner Laszlo Hanyecz bot in einem Internetforum 10.000 Bitcoins für zwei Pizzen. Nach drei Tagen bestellte ein Engländer bei einem amerikanischen Pizzaservice zwei Pizzen für Laszlo und bezahlte diese mit seiner Kreditkarte. Laszlo hielt daraufhin sein Versprechen und transferierte 10.000 Bitcoins an den Engländer.⁸

Bis heute konnte nicht zweifelsfrei geklärt werden, wer genau hinter der Entwicklung der neuen Zahlungsmethode Bitcoin steckt. Viele Recherchen und Versuche von

⁷ Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S.13

⁸ Specht, P., Die 50 wichtigsten Themen der Digitalisierung, München 2018, S.211ff

Journalisten konnten die Identität der Person oder Gruppen hinter dem Pseudonym Satoshi Nakamoto nicht zweifelsfrei aufdecken.⁹

Ausgehend von der Bitcoin-Blockchain wurden immer mehr unterschiedliche Blockchains entwickelt. Durch Veränderung vorhandener Prozesse und Ergänzung von Funktionen entstanden viele verschiedene, die auf bestimmte Anwendungsfälle zugeschnitten sind und eigene Ziele und Ideologien verfolgen. So entstanden viele weitere Kryptowährungen, die sogenannten Altcoins (alternativen Coins), mit ihren eigenen, individuell gestalteten Blockchains wie bspw. Ethereum mit der Kryptowährung Ether. Aber auch Blockchains, die völlig ohne eine Kryptowährung arbeiten und nicht die Abwicklung von Finanztransaktionen als Grundlage haben, wurden in verschiedensten Branchen konzipiert und sollen dort für nicht weniger als eine Revolution der Geschäftsprozesse sorgen. Allen Entwicklungen bleibt jedoch eine dezentrale, unveränderliche Datenbank, die ohne vermittelnde Instanz arbeitet, als Grundlage gemein.¹⁰

2.2 Die Funktionsweise der Blockchain – Technologie

Um besser zu verstehen wie eine Blockchain aufgebaut ist und funktioniert, werde ich in diesem Abschnitt die Grundlagen und Fachbegriffe erläutern, die für das Verständnis der Prozesse nötig sind. Auf zu spezifische und technische Details werde ich dabei verzichten, da der Fokus auf dem grundlegenden Verständnis liegt. Blockchains können in ihrer genauen Funktionsweise variieren und je nach Verwendungszweck vielfältig angepasst werden. Ausgehend von der Kryptowährung Bitcoin, die die erste und populärste Blockchain nutzt, werde ich auch auf andere technische Umsetzungen und Möglichkeiten eingehen, jedoch ohne sämtliche Varianten aufzuführen.

⁹ Specht, P., Die 50 wichtigsten Themen der Digitalisierung, München 2018, S.220f

¹⁰ Ebd., S.219f

2.2.1 Grundlagen

Zunächst gebe ich zwei Definitionen des Begriffs Blockchain:

„Eine Blockchain ist eine vollständige und unveränderliche Historie zu allen Transaktionen einer dezentralen Community, der jeder, der ein Teil davon ist, zustimmt.“¹¹

Oder auch

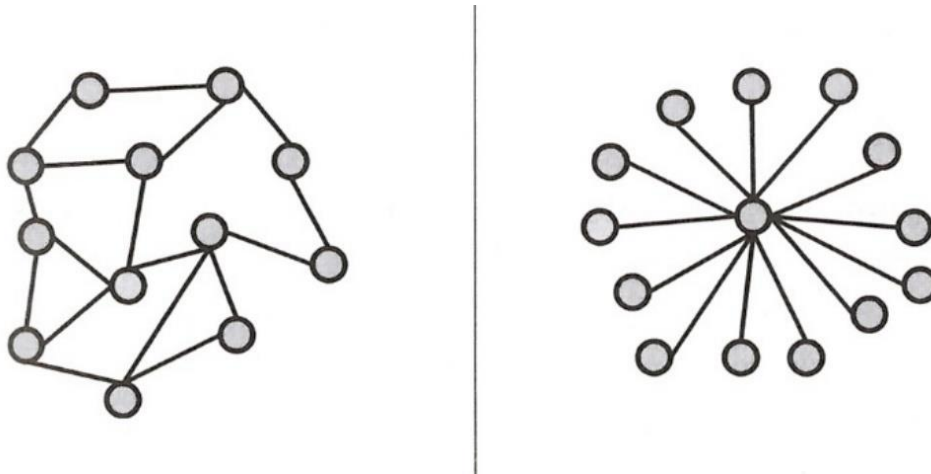
„ein rein verteiltes Peer-to-Peer-System von Hauptbüchern, das eine Softwarekomponente verwendet, die aus einem Algorithmus besteht, der den Informationsgehalt geordneter und verbundener Datenblöcke gemeinsam mit kryptographischen und Sicherheitstechnologien aushandelt, um dessen Integrität zu erreichen und zu erhalten.“¹²

Eine Blockchain besteht also aus kryptografisch miteinander verketteten, und damit vor nachträglichen Veränderungen geschützten Datenblöcken, auf deren Inhalt sich die Nutzer eines Netzwerkes zuvor geeinigt haben. Sie wird nicht an einem zentralen Ort wie bspw. einem Server gespeichert und verwaltet, sondern bei vielen Nutzern als identische Kopie hinterlegt. Durch die dezentrale Struktur des Netzwerkes gibt es für Angreifer kein eindeutiges Ziel. Störungen, Ausfälle oder Abschaltung einzelner Teilnehmer können einfach kompensiert werden, indem auf Verbindungen zu anderen Teilnehmern ausgewichen wird. Auch vor Datenverlust schützt die vielfache, dezentrale Speicherung.

¹¹ Hosp, J., Kryptowährungen, München 2018, S.45

¹² Drescher, D., Blockchain Grundlagen, Frechen 2017, S.55

Folgende Abbildung zeigt schematisch den unterschiedlichen Aufbau von zentralen und dezentralen Netzwerken.



*Abbildung 1 Dezentrales (links) und zentrales (rechts) Netzwerk im Vergleich
Drescher, D., Blockchain Grundlagen, Frechen 2017, S.31*

Da es keine zentrale Institution gibt, die über die Gültigkeit von beispielsweise Transaktionen entscheidet, wird asymmetrische Verschlüsselung genutzt um eine korrekte Autorisierung der Teilnehmer bei Transaktionen sicherzustellen.

Die Abbildung auf der nächsten Seite zeigt die Funktionsweise von asymmetrischer Kryptographie. Dabei wird ein Schlüsselpaar bestehend aus einem öffentlichen Schlüssel (auch Public Key, in weiß dargestellt) und einem privaten Schlüssel (auch Private Key, in schwarz dargestellt) genutzt.

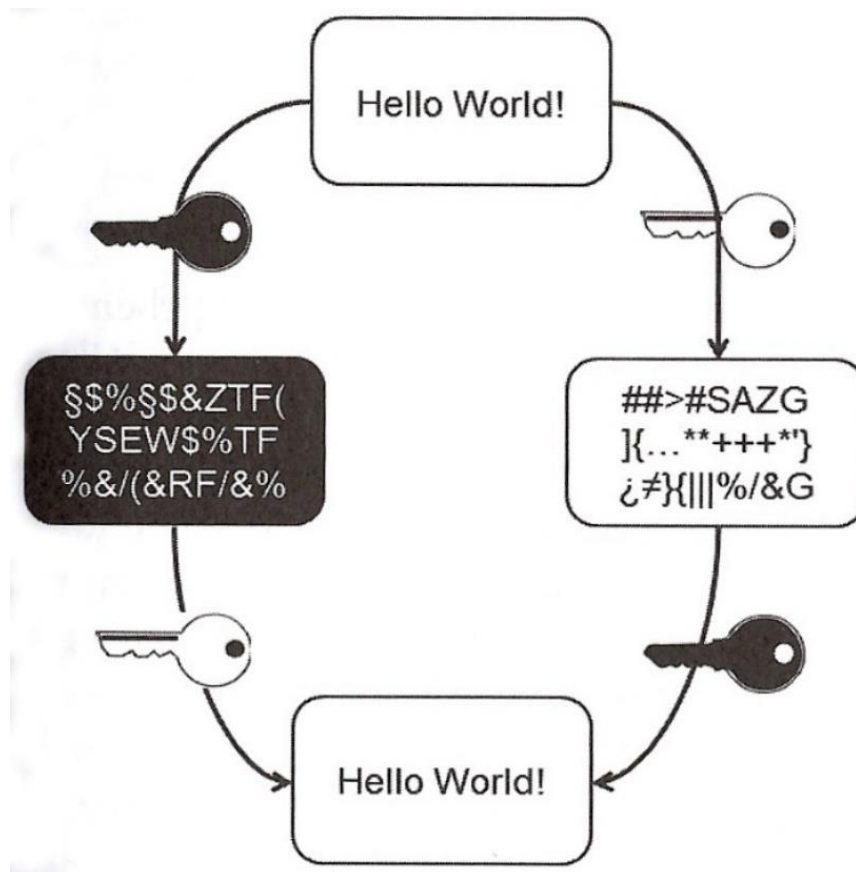


Abbildung 2 Veranschaulichung von asymmetrischer Kryptographie
Drescher, D., Blockchain Grundlagen, Frechen 2017, S.115

Für die Verschlüsselung von Daten, hier dem Text ‚Hello World!‘, wird ein kryptographischer Schlüssel verwendet. Um den Text wieder zu entschlüsseln, muss der andere Schlüssel des Schlüsselpaars genutzt werden. Eine Entschlüsselung mit demselben Schlüssel, mit dem die Daten zuvor verschlüsselt wurden, ist nicht möglich, da es sich bei dem genutzten kryptographischen Verfahren um eine Einwegfunktion handelt. Ebenso wurde das Schlüsselpaar mit einer Einwegfunktion erstellt. Der Public Key wurde dazu aus dem Private Key erstellt. Aus dem bekannten Public Key kann also niemand den Private Key errechnen. Die Bezeichnungen Public- und Private Key kommen daher, dass der Private Key tatsächlich niemals vom Nutzer weitergegeben wird. Der Public Key repräsentiert im Blockchain-Netzwerk die Kontonummer des Nutzers und ist anderen Teilnehmern daher bekannt. In der Praxis kann der Teilnehmer mit seinem Private Key verschlüsselte Nachrichten erstellen, die von anderen Teilnehmern mit seinem Public Key wieder entschlüsselt werden können. Bei erfolgreicher Entschlüsselung ist also eindeutig, dass die Nachricht von dem Teilnehmer stammt,

dessen Public Key zur Entschlüsselung genutzt wurde. Umgekehrt können andere Teilnehmer den Public Key nutzen, um dem Teilnehmer eine Nachricht zu senden, die nur von ihm mit seinem Private Key entschlüsselt werden kann.

Dieses Verfahren wird genutzt, um Transaktionen mittels digitaler Signatur zu autorisieren. Die folgende Abbildung veranschaulicht die Erstellung und Überprüfung einer digitalen Signatur mithilfe von asymmetrischer Kryptographie.

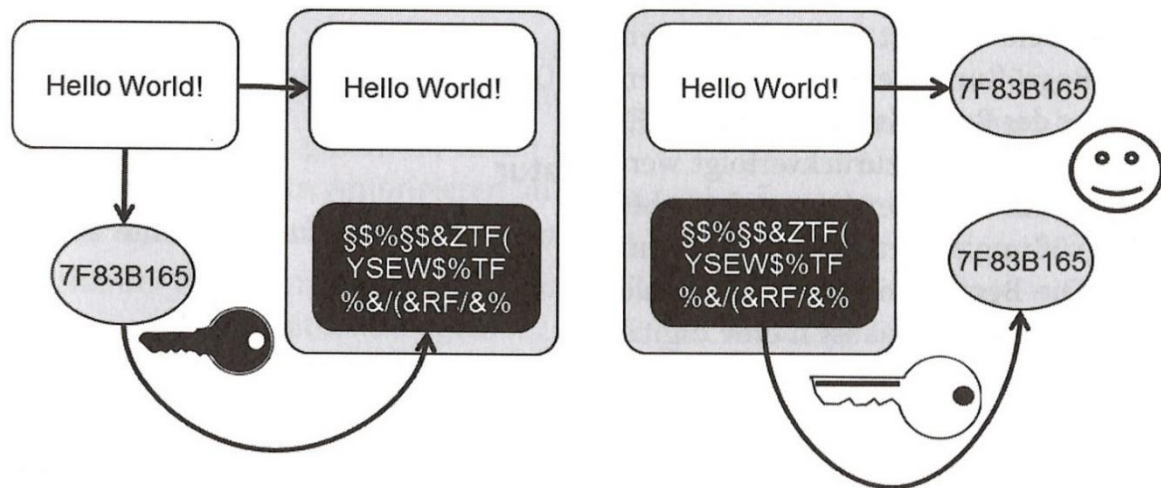


Abbildung 3 Erstellung und Überprüfung einer digitalen Signatur mithilfe asymmetrischer Verschlüsselung

eigenes Werk in Anlehnung an Drescher, D., Blockchain Grundlagen, Frechen 2017, S. 123f

Um eine autorisierte Nachricht oder auch Transaktion zu erstellen, verfasst der Absender diese. Zusätzlich ermittelt er einen sogenannten Hashwert (siehe Kapitel 2.2.2) für diese Nachricht und verschlüsselt diesen mit seinem Private Key. Beides zusammen schickt er dann an das Netzwerk. Die anderen Teilnehmer können die korrekte Autorisierung nun überprüfen, indem sie ihrerseits den Hashwert der erhaltenen Nachricht berechnen. Anschließend entschlüsseln sie die Signatur mit dem Public Key des Absenders und vergleichen die beiden Werte. Stimmen die Werte überein, so haben sie denselben Klartext erhalten, den der Absender verfasst hat und dessen Hashwert er zuvor verschlüsselt hat. Die Nachricht ist also echt, korrekt autorisiert und inhaltlich nicht manipuliert worden. Weichen die Werte beim

Empfänger jedoch voneinander ab, so wurde der Inhalt der Nachricht manipuliert und ein Betrugsversuch erkannt.¹³

Die Teilnehmer eines solchen Blockchain-Netzwerkes teilen sich meist in die Gruppen der **User**, **Nodes** und **Miner** auf. Dabei müssen sich die Teilnehmer nicht zwangsläufig auf eine einzelne Funktion beschränken, sondern können auch mehrere Funktionen übernehmen.

User nutzen, wie der Name schon sagt, das Netzwerk lediglich und beteiligen sich nicht aktiv am Betrieb von diesem. Beispielsweise tätigen sie nur Zahlungen oder empfangen diese. Sie speichern weder eine Kopie der Blockchain noch beteiligen sie sich an der Verifizierung von Transaktionen. Bei Kryptowährungen stellen die User in der Regel die größte Teilnehmergruppe.

Nodes (Knotenpunkte) hingegen erhalten diese Transaktionen von den Usern, überprüfen diese auf korrekte Autorisierung und leiten sie an die anderen Nodes im Netzwerk weiter. Ebenso speichert jeder Node die gesamte Blockchain und stellt so die dezentrale Verfügbarkeit sicher. Der Ausfall eines einzelnen Nodes oder die Manipulation der bei ihm gespeicherten Blockchain hat praktisch keine Auswirkungen auf den Betrieb des Netzwerkes, da die Informationen vielfach verfügbar sind und eine einzelne abweichende Variante der Blockchain schnell als manipuliert erkannt und von den anderen Nodes für ungültig erklärt werden kann.

Miner bilden die letzte Gruppe der Teilnehmer. Sie verifizieren die von den Usern gemachten Transaktionen, indem sie diese in einen Block eintragen und Konsensus erzeugen. Für Belohnung für diese Tätigkeit erhalten die Miner zum einen von den Usern gezahlte Transaktionsgebühren und im Falle von Bitcoin auch noch eine festgelegte Anzahl an Bitcoins aus einem endlichen Vorrat. In Anlehnung an das Schürfen von Gold kommt daher auch die Bezeichnung Miner, da sie diesen Vorrat quasi abbauen.¹⁴ Bei Bitcoin beträgt die festgelegte Belohnung derzeit 12,5 Bitcoins für jeden erstellten Block. Alle vier Jahre halbiert sich diese Belohnung. Im Jahr 2130 werden schließlich alle Bitcoins geschürft und damit im Umlauf sein, da die

¹³ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.112ff

¹⁴ Hosp, J., Kryptowährungen, München 2018, S.60f

maximale Anzahl auf 21 Millionen begrenzt ist. Ein Nachdrucken, wie bei herkömmlichen Währungen möglich, ist nicht vorgesehen.¹⁵

Die Verwaltung und Zuordnung von Eigentum und die Dokumentation von Transaktionen einer Kryptowährung sind zwar Anwendungsfälle, für die die Blockchain-Technologie prädestiniert ist und ursprünglich entwickelt wurde, jedoch ist sie keineswegs auf dieses Anwendungsgebiet beschränkt. In den Datenblöcken können nicht nur Transaktionsdaten, sondern Informationen jeglicher Art gespeichert und im Netzwerk verfügbar gemacht werden.

2.2.2 Hashing

Hashing ist ein zentraler Bestandteil der Blockchain-Technologie. „Hashfunktionen sind kleine Computerprogramme, die beliebige Daten ungeachtet des Umfangs der Eingabedaten als eine Zahl mit fester Länge abbilden.“¹⁶ Die Anwendung beschränkt sich also nicht nur auf Textdateien. Die ausgegebenen Hashwerte weisen dabei die folgenden vier Eigenschaften auf:

- Die Hashwerte sind **deterministisch**, die Hashfunktion liefert auch bei mehrfacher Ausführung bei gleichen Eingabedaten jedes Mal den gleichen Hashwert.
- Der Ergebniswert ist dabei **pseudozufällig**. Wie zuvor geschrieben erzeugen die gleichen Eingabedaten jedes Mal den gleichen Hashwert. Ändert man jedoch die Eingabedaten, so lässt sich nicht vorhersagen, wie sich der Hashwert ändert. Selbst kleine Veränderungen in den Eingabedaten können einen völlig anderen Hashwert erzeugen.
- Da es nicht möglich ist zu berechnen, welche Eingabedaten nötig sind um einen bestimmten Hashwert zu erhalten, handelt es sich hierbei um eine **Einwegfunktion**.

¹⁵ Specht, P., Die 50 wichtigsten Themen der Digitalisierung, München 2018, S.218

¹⁶ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.89, zitiert nach Weisstein, E. W., Hash function, in: <http://mathworld.wolfram.com> (abgerufen am 26.09.2018)

- Zuletzt sind Hashfunktionen nahezu **kollisionsresistent**. Das bedeutet, dass verschiedene Eingabedatensätze nicht einen identischen Hashwert erzeugen können. So wird sichergestellt, dass stets eine eindeutige Zuordnung der Werte möglich ist, ähnlich wie Fingerabdrücke oder DNA-Spuren eindeutig einem bestimmten Menschen zugeordnet werden können.¹⁷

Diese Eigenschaften sorgen dafür, dass die Daten in einer Blockchain praktisch unveränderbar sind. Wie dies gewährleistet wird, veranschaulicht die folgende Abbildung.

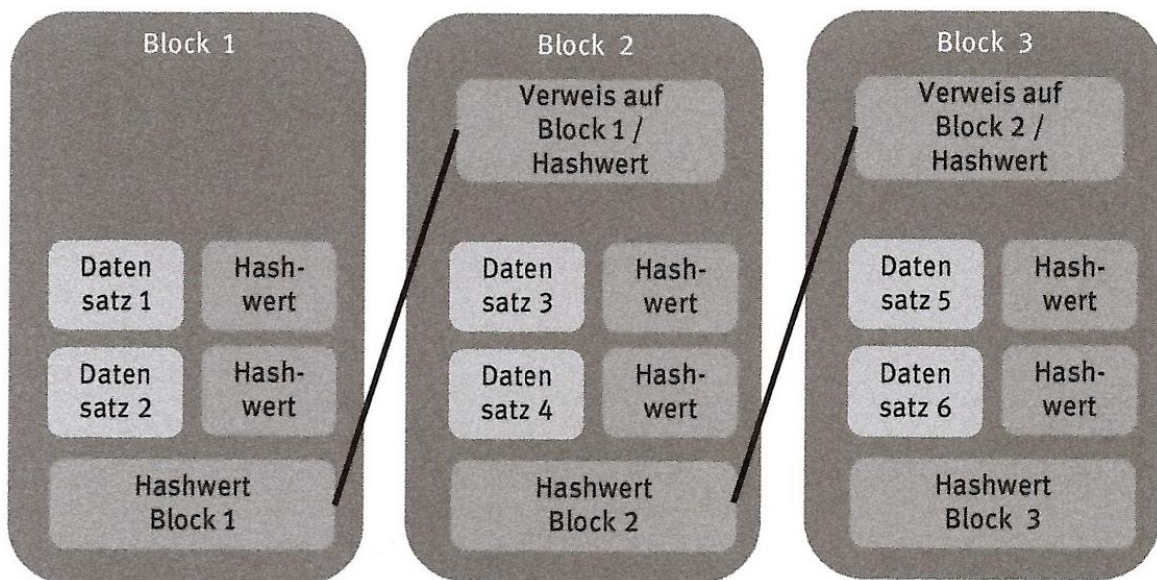


Abbildung 4: Vereinfachte Darstellung der Verkettung der einzelnen Blockchain-Blöcke
 Burgwinkel, D., *Blockchaintechnologie und deren Funktionsweise verstehen*, in: Daniel Burgwinkel
 (Hrsg.) *Blockchain Technology*, Berlin/Boston 2016, S.6

Von den in den Blöcken enthaltenen Daten wird der Hashwert ermittelt und in den sogenannten Block-Header geschrieben. Jeder folgende Block der Blockchain enthält einen Verweis auf den Hashwert des vorherigen Blocks. Die einzelnen Blöcke sind auf diese Weise eindeutig miteinander verbunden und die gesamte Historie kann bis zu ihrem Ursprung zurückverfolgt werden. Da die Hashwerte im Header vom Inhalt der jeweiligen Blöcke abhängig sind, führt eine manipulative

¹⁷ Drescher, D., *Blockchain Grundlagen*, Frechen 2017, S.89ff

Veränderung der enthaltenen Daten wie zum Beispiel bei Transaktionen bei einer Änderung der Summe oder des Empfängers einer Zahlung dazu, dass sich der Hashwert im Block-Header verändert. In der Folge stimmt die Verkettung der Blöcke nicht mehr, da der folgende Block einen anderen Hashwert im Header seines Vorgängers ausweist. Ein Versuch, diese so manipulierte Blockchain im Netzwerk zu verbreiten, würde scheitern, weil durch diesen Bruch in der Kette die Datenmanipulation schnell zu erkennen ist. Die betroffene Blockchain würde im Netzwerk nicht akzeptiert werden. Um trotz manipulierter Daten wieder eine korrekte Blockchain zu erstellen, müsste der Verweis des folgenden Blocks geändert werden. Da dieser Verweis aber zum Inhalt zählt, aus dem der Hashwert des Blocks berechnet wird, entsteht wieder ein Bruch in der Kette. In der Folge müssten sämtliche dem veränderten Block folgenden Blöcke neu berechnet werden. Erst wenn die durchgängig korrekte Verknüpfung der Blöcke wiederhergestellt ist, bestünde überhaupt die Möglichkeit, die manipulierte Blockchain im Netzwerk zu etablieren.¹⁸ Dabei ist zu beachten, dass die ursprüngliche, nicht manipulierte Blockchain in der Zeit immer weiter wächst, da alle anderen Teilnehmer des Netzwerkes weiterhin an dieser arbeiten. Dieser Rückstand müsste zusätzlich aufgeholt werden, da das Netzwerk die längste korrekte Blockchain als die richtige betrachtet. Erschwert wird das Aufholen dadurch, dass die Berechnung und Bildung der Blockchain an bestimmte Bedingungen geknüpft ist. Solch eine Manipulation der Transaktionshistorie wäre überhaupt nur möglich, wenn der Angreifer die Mehrheit unter den Minern im Netzwerk kontrolliert. Eine solche Attacke auf das Netzwerk wird daher auch als 51-Prozent-Angriff bezeichnet.¹⁹ In der Theorie ist so ein Angriff zwar möglich, bei einigermaßen großen Netzwerken technisch aber nur schwer realisierbar. Beachtet werden müssen auch die Kosten für einen solchen Angriff, die dafür sorgen können, dass der Manipulationsversuch wirtschaftlich unrentabel ist.²⁰

Warum das Erstellen einer neuen Blockchain so aufwendig sein kann und wie das Netzwerk entscheidet, was in einem Block erfasst wird und welcher Block in die Blockchain integriert wird, werde ich im nächsten Punkt erläutern.

¹⁸ Drescher, D., Blockchain Grundlagen, Frechen 2017, S. 130ff

¹⁹ Ebd. S.192f

²⁰ Hosp, J., Kryptowährungen, München 2018, S.119

2.2.3 Konsens-Mechanismen

Da in einer Blockchain keine zentrale Institution Entscheidungen trifft, muss sich die Gemeinschaft selbst einigen. Dafür muss Konsensus erzeugt werden, das „bedeutet Zustimmung und ist die Einigung darüber, was passiert ist und was nicht.“²¹

Bei einer Blockchain, welche für eine Kryptowährung eingesetzt wird, sieht das wie folgt aus: Ein User tätigt eine Transaktion, d.h. er überträgt einem anderen User das Eigentum an einem Teil der ihm gehörenden Coins. Die Transaktion wird über das Netzwerk an die Nodes verteilt. Wie bei einer normalen Überweisung bei einer Bank muss auch hier geprüft werden, ob die Transaktion gültig ist. Es muss sichergestellt sein, dass der angegebene Absender auch tatsächlich diese Transaktion autorisiert hat, ihm ausreichend viele Coins zur Verfügung stehen und ein korrekter, existierender Empfänger angegeben wurde. Er muss mit dem zu seiner Public Address passenden Private Key signiert haben und seiner Public Address muss eine ausreichende Menge an Coins zugeordnet sein. Ist die angegebene Public Address des Empfängers nun auch noch korrekt, so kann die Transaktion in die Blockchain aufgenommen werden. Kryptographische Regeln sorgen dabei dafür, dass die Daten der Transaktion nicht verändert und verfälscht werden können. An die genutzten Algorithmen werden dabei folgende Anforderungen gestellt:

1. Es dürfen keine Informationskonflikte auftreten, falls bspw. innerhalb sehr kurzer Zeit versucht wurde die gleiche Transaktion an zwei verschiedene Empfänger zu tätigen. Wenn in diesem Fall unterschiedliche Miner jeweils Transaktion A oder B als korrekt akzeptieren wollen, muss gewährleistet werden, dass nur eine Transaktion in die Blockchain aufgenommen wird.
2. Um als Miner tätig und an der Konsensbildung beteiligt zu sein, müssen dem Teilnehmer in irgendeiner Form Kosten entstehen. Es darf einzelnen Teilnehmern nicht ohne Weiteres möglich sein, eine große Anzahl an Minern zu erstellen und an der Konsensbildung teilnehmen zu lassen. Sie würden damit die Chancen erhöhen, dass einer ihrer Miner den nächsten Block mit gültigen Transaktionen erstellt, und könnten mit einer entsprechenden Mehrheit die restlichen Teilnehmer des Netzwerkes überstimmen. Dies

²¹ Hosp, J., Kryptowährungen, München 2018, S.60

würde zu einer zunehmenden Zentralisierung führen, welche ja gerade vermieden werden soll.

3. Finanzielle Anreize müssen auf der anderen Seite dafür sorgen, dass trotz der Kosten viele Teilnehmer bereit sind als Miner aktiv zu sein und damit für eine Dezentralisierung im Netzwerk sorgen.²²

Letztendlich muss es ein Verfahren geben, nach welchem ermittelt wird, welcher der vielen am Netzwerk beteiligten Miner den nächsten Block an die Blockchain anhängen darf und den enthaltenen Transaktionen damit Gültigkeit verleiht. Auch wenn immer mehr Modelle zur Schaffung von Konsensus entstehen, „haben sich die folgenden drei Möglichkeiten als Konsensus-Mechanismen entweder in Kombination oder alleine bewährt:

1. Proof of Importance (zu Deutsch: Wichtigkeitsnachweis)
2. Proof of Stake (zu Deutsch: Geldnachweis)
3. Proof of Work (zu Deutsch: Arbeitsnachweis)²³

Um beim **Proof of Importance** die Wichtigkeit eines Teilnehmers zu bewerten, kann zum Beispiel die Zeitspanne, seit der er Teil des Netzwerks ist, herangezogen werden. Ebenso kann die Anzahl anderer Teilnehmer, die sich mit ihm vernetzt haben, ein Kriterium für dessen Wichtigkeit sein. Lange mitwirkende und gut etablierte Teilnehmer erhalten so eine höhere Wertschätzung und Vertrauen als später hinzugekommene und weniger gut vernetzte. Je höher die Wichtigkeit eines Teilnehmers im Netzwerk eingestuft wird, desto größer ist die Wahrscheinlichkeit, dass er den nächsten Block erstellen darf. Eine Schwachstelle ergibt sich jedoch bei offenen Netzwerken ohne Zugangsbeschränkung für neue Teilnehmer, in denen es keine Kostenhürde für deren Hinzufügen existiert. In betrügerischer Absicht könnte eine Person eine größere Anzahl an Teilnehmern erstellen und miteinander vernetzen, um deren Wichtigkeit im Netzwerk zu erhöhen. Der Ersteller dieser vielen Teilnehmer würde so deutlich seine Chancen verbessern, über die Konsensbildung entscheiden zu dürfen. Aktuell ist der Proof of Importance daher die „am wenigsten

²² Hosp, J., Kryptowährungen, München 2018, S.62f

²³ Ebd. S.64

verwendete Methode zur Konsensbildung“.²⁴ Mit einigen Anpassungen und zusätzlichen Funktionen könnte sich dies aber in Zukunft ändern.²⁵

Beim **Proof of Stake** wird Wichtigkeit mit Geld gleichgesetzt. „Wer mehr Geld im System kontrolliert, bekommt automatisch eine größere Bedeutung.“²⁶ Dieser kapitalistische Ansatz wird häufig kritisiert, da die reichsten Teilnehmer mit den meisten Stimmanteilen und damit auch den größten Anteilen an den Prämien belohnt werden. Ebenso besteht die Gefahr der Zentralisierung der Stimmanteile bei einigen wenigen Teilnehmern. Bisher setzen daher nur wenige Blockchains den Proof of Stake ein. Grundsätzlich funktioniert das System dort allerdings gut. Als ein Vorteil gilt die Kalkulierbarkeit von Stimm- und Gewinnanteil. Dazu setzt man das eigene Kapital mit dem Gesamtkapital des Netzwerks ins Verhältnis. So lässt sich die erzielbare Rendite ermitteln, allerdings unter der Voraussetzung, dass sich das Verhältnis und der Gegenwert nicht bedeutend verändern. Ebenso ist ein bösartiger Angriff auf das Netzwerk nicht einfach durch das Erstellen vieler Teilnehmer möglich. Stimmanteile können nicht aus dem ‚Nichts‘, sondern nur durch tatsächlich vorhandenes und ins Netzwerk eingebrachte Geld erreicht werden.²⁷

Der dritte Mechanismus um Konsens zu erzielen ist der **Proof of Work**. Dabei ist er sowohl der älteste als auch der am weitesten verbreitetste. Hier darf derjenige Miner die Blockchain um einen Block erweitern, der als erstes nachweisen kann, dass er bzw. seine Computerhardware eine bestimmte Arbeit geleistet hat. Die Arbeit sieht dabei wie folgt aus. Der Miner sammelt Transaktionen für einen Block und ermittelt für diesen anschließend den Hashwert. Dieser muss jedoch bestimmten Bedingungen entsprechen. Bei Bitcoin muss der Wert mit einer bestimmten Anzahl an Nullen beginnen. Je mehr Nullen gefordert sind, desto größer ist die sogenannte Mining Difficulty. Diese Schwierigkeit wird immer wieder angepasst, damit es immer etwa zehn Minuten dauert, um einen neuen Block zu erstellen, auch wenn sich die gesamte im Netzwerk verfügbare Leistung verändert. Gemessen wird diese Leistung in der Anzahl an Versuchen (Hashes) pro Zeiteinheit, der sogenannten Hash-Rate. Um einen Hashwert zu erreichen, der den geforderten Bedingungen

²⁴ Hosp, J., Kryptowährungen, München 2018, S.63

²⁵ Ebd., S.63f

²⁶ Ebd., S.66

²⁷ Ebd., S.66f

entspricht, muss der Miner eine sogenannte Nonce finden. Dies ist ein im Block enthaltener variabler Wert, der vom Miner frei gewählt werden kann. Da es durch die Verwendung einer Einwegfunktion nicht möglich ist vom gesuchten Hashwert aus die unbekannte Nonce zu berechnen, bleibt nur die Möglichkeit so lange verschiedene Noncen auszuprobieren, bis ein passender Hashwert für den gesamten Block gefunden wurde.²⁸ Ist eine passende Nonce gefunden, wird der fertige Block im Netzwerk verbreitet, von den anderen Teilnehmern nach Prüfung akzeptiert und an die Blockchain angehängt. Anschließend beginnt dieser Ablauf mit dem nächsten Block von vorne.

Für die Berechnung solcher Noncen können theoretisch normale handelsübliche Computer eingesetzt werden. Bei Bitcoin ist die Gesamtleistung des Netzwerkes allerdings inzwischen so groß, dass selbst leistungsstarke handelsübliche Computer kaum mehr eine Rolle spielen. Zum Vergleich: Im Bitcoin-Netzwerk lag die durchschnittliche Hashrate am 22.09.2018. bei über 55 Trillionen Hashes pro Sekunde.²⁹ Mit einem handelsüblichen PC und aktueller Hardware lassen sich etwa 30 bis 50 Millionen Hashes erreichen. Der Anteil der eigenen Rechenleistung im gesamten Bitcoin-Netzwerk ist damit so gering, dass die Chancen, als erster einen passenden Block zu erstellen, verschwindend niedrig sind. Stattdessen kommen spezialisierte Rechner, sogenannte ASIC-Miner (application-specific integrated circuit, zu Deutsch: anwendungsspezifischer integrierter Schaltkreis), zum Einsatz. Diese Computer sind ausschließlich auf Hashing ausgelegt. Eine anderweitige Verwendung ist nicht möglich. Abgesehen davon, dass Konsensus erzeugt wird, sind die geleisteten Berechnungen allerdings sinnlos und bieten keinen weiteren Mehrwert. Die Kritik von Umweltschützern, die eine gigantische Stromverschwendung sehen, ist also durchaus berechtigt.³⁰ Exakt berechnen lässt sich der Stromverbrauch des dezentralen Bitcoin-Netzwerkes nicht. Dazu ist zu viel unterschiedliche Hardware mit stark variierender Energieeffizienz beteiligt, über deren Verwendungshäufigkeit keine Daten existieren. Eine Berechnung mit groben Schätzwerten kommt für Oktober 2017 auf einen Energieverbrauch von 343

²⁸ Hosp, J., Kryptowährungen, München 2018, S.67f

²⁹ BitInfoCharts, Bitcoin Hashrate historical chart, in: <https://bitinfocharts.com>, (abgerufen am 23.09.2018)

³⁰ Hosp. J., Kryptowährungen, München 2018, S.76f

Megawatt pro Sekunde. So viel verbrauchen 98 durchschnittliche Haushalte in Deutschland in einem ganzen Jahr.³¹ Die Speicherung von Daten in der Bitcoin-Blockchain gilt heute als „die vermutlich teuerste Form von Datenspeicherung, die je erfunden wurde.“³² Es gibt daher bereits erste Ansätze „DNA-Rekombinations-Berechnungen, Primzahlrecherchen und einiges mehr“³³ in diesen Prozess zu integrieren. Damit könnten die geleisteten Berechnungen mehr als nur einen Arbeitsnachweis darstellen. Solche Funktionen befinden sich derzeit aber noch in der Implementierung, da sie natürlich auf die Anforderungen an eine Blockchain angepasst werden müssen.³⁴

2.2.4 Smart Contracts

Als Smart Contracts bezeichnet man kleine, ausführbare Programme, welche auf der Blockchain hinterlegt sind. Einmal in die Blockchain aufgenommen, lässt sich der Inhalt eines Smart Contracts nicht mehr verändern.³⁵ Eine so erweiterte Blockchain speichert nicht mehr nur Transaktionen, sondern kann auch selbst zuvor vereinbarte Transaktionen ausführen. Der Begriff Smart Contract lässt sich daher am besten als ‚selbstaussführende Verträge‘ ins Deutsche übersetzen.³⁶ Die Funktion im Programmcode ist nach dem wenn-/dann-Schema aufgebaut. Wenn ein bestimmtes Ereignis oder eine Eingabe erfolgt ist, dann wird ein zugehöriges Folgeereignis ausgelöst. Das Prinzip von Smart Contracts ist nicht neu und wird in analoger Form schon lange im Alltag genutzt. Die Funktionsweise lässt sich einfach am Beispiel eines Verkaufsautomaten erklären. Wenn genug Geld eingeworfen wurde, dann wird ein Produkt ausgegeben. Der Automat ersetzt den Mittelsmann, also in diesem Beispiel den Verkaufsangestellten, zwischen Käufer und eigentlichem Verkäufer. Für den Käufer ergibt sich der Vorteil, dass er an keine Öffnungszeiten gebunden ist. Der Bestücker des Automaten profitiert von geringeren Kosten für den Automaten als für einen menschlichen Mittelsmann.

³¹ Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S.124

³² Ebd., S.121

³³ Hosp, J., Kryptowährungen, München 2018, S.80

³⁴ Ebd., S.80

³⁵ Kienzler, R., Hyperledger – eine offene Blockchain Technologie, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology, Berlin/Boston 2016, S. 118

³⁶ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.249f

Dieses Prinzip des Vertragsschlusses lässt sich einfach in eine digitale Form übertragen, der Smart Contract auf der Blockchain ersetzt den Verkaufsautomaten aus dem Beispiel. Die beteiligten Parteien legen Bedingungen fest, welche Eingaben zu welchen Ausgaben führen sollen. Diese werden in eine Programmiersprache übersetzt und als Smart Contract in der Blockchain gespeichert.

Von da an ist der Programmcode aktiv und wird auf Ereignisse mit entsprechenden Ausgaben reagieren. Ein manuelles Starten oder Bestätigen ist nicht mehr erforderlich. Eine einseitige, nachträgliche Veränderung oder Verweigerung der vereinbarten Leistung ist ab diesem Zeitpunkt ebenfalls nicht mehr möglich, da die Eigenschaften der Blockchain ebendies verhindern.³⁷

Doch nicht jede Blockchain eignet sich für den Einsatz von Smart Contracts. Die Bitcoin-Blockchain unterstützt keine Smart Contracts³⁸ und die Blockchain Ethereum bietet keine Möglichkeit aus Smart Contracts auf externe Anwendungen zuzugreifen. Außerhalb der Blockchain liegende Daten können nicht abgerufen werden, sondern müssen vollständig in den Smart Contract integriert werden, was diesen unter Umständen sehr komplex macht.³⁹ Voraussetzung für alle Anwendungsbeispiele ist natürlich ebenso eine rechtlich verbindliche Gültigkeit und Akzeptanz der Eintragungen auf der Blockchain, welche heute noch nicht zutrifft.⁴⁰

Sobald aber rechtliche Gültigkeit und Verknüpfungsmöglichkeiten gegeben sind, ergeben sich diverse Anwendungsmöglichkeiten. Für das folgende Beispiel wird daher angenommen, dass Kaufverträge auf der Blockchain als rechtlich bindend angesehen werden bzw. das gültige Grundbuch in die Blockchain integriert wurde.

Ein Hauskauf könnte dann vollständig ohne Einbindung eines Notars als vertrauenswürdige Instanz zwischen Käufer und Verkäufer erfolgen. Sobald der Kaufpreis bezahlt wurde, wird das Eigentum an der Immobilie automatisch übertragen. Der Smart Contract registriert dazu die Zahlung des Käufers an den

³⁷ Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S.97ff

³⁸ Merz, M., Einsatzpotenziale der Blockchain im Energiehandel, in: Daniel Burgwinkel (Hrsg.) Blockchain Technology, Berlin/Boston 2016, S.58

³⁹ Ploom, T., Blockchains - wichtige Fragen aus IT-Sicht, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology, Berlin/Boston 2016, S.144

⁴⁰ Ploom, M., Blockchain Business Modelle in der Finanzindustrie, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology, Berlin/Boston 2016, S.100

Verkäufer. Ist die vereinbarte Summe erreicht, wird das Eigentum an der Immobilie übertragen. Die Blockchain hat dabei die Funktion eines digitalen Grundbuchs. Der Käufer kann darauf vertrauen, das Eigentum übertragen zu bekommen, sobald er bezahlt hat. Er muss sich keine Gedanken machen, ob er dem Verkäufer selbst auch vertrauen kann und dieser ihm nach Zahlung auch wirklich das Eigentum überträgt. Das Vertrauen erhält hier die Blockchain und die verwendeten Algorithmen.

Smart Contracts können allerdings auch deutlich komplexere Formen annehmen und sind nicht nur auf Transaktionen nach dem Schema Geld gegen Ware beschränkt. Für jede Vereinbarung, die sich in der wenn-/dann-Schreibweise formulieren lässt, kann ein Smart Contract erstellt werden. Eine Spedition könnte beispielsweise für eine flexible Rate LKWs leasen. Für eine bestimmte Laufleistung ist dann automatisch eine bestimmte Leasingrate fällig. Die Fahrzeuge rechnen die Nutzung im Rahmen der Vereinbarung quasi selbst ab. Ebenso kann an die ordnungsgemäße Bezahlung der Rate das Eigentum an den Fahrzeugen gebunden und in der Blockchain hinterlegt sein.

Smart Contracts kontrollieren und führen sich selbst aus, das unterscheidet sie von gewöhnlichen Verträgen und macht sie ‚smart‘. Niemand muss die Einhaltung überwachen oder könnte bestochen werden. Einmal geschlossen und in der Blockchain erfasst, sind die Bedingungen gültig und führen sich beim Eintritt automatisch aus. Eine Manipulation oder nachträgliche Veränderung ist ausgeschlossen. Es gelten exakt die anfänglich vereinbarten Bedingungen. Allerdings müssen die vertragsschließenden Parteien in diesem Fall auch selbst überprüfen, ob die vereinbarten Bedingungen und Klauseln auch geltendem Recht entsprechen und korrekt formuliert wurden. Der intermediäre Experte ist schließlich nicht mehr vorhanden.

Die Möglichkeit Verträge so einfach mit großer Zuverlässigkeit zu schließen, die Möglichkeiten für Betrugsversuche und die damit zusammenhängenden Kosten zu minimieren, sowie den Weg über Notare, Banken und andere Mittelsmänner zu sparen, macht diese Verträge so attraktiv für Unternehmen.⁴¹

⁴¹ Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S.97ff

2.2.5 Öffentliche und private Blockchains

Die Bitcoin-Blockchain ist frei für jeden neuen User zugänglich, der Teil des Netzwerks werden möchte. Es bedarf keines Antrages auf Mitgliedschaft oder einer Bonitätsprüfung und es existiert keine Instanz, die neue User ablehnen könnte. Man spricht in diesem Fall von einer ‚Public Blockchain‘, also ein öffentlich im Internet erreichbares System.

Für bestimmte Einsatzszenarien kann es jedoch erforderlich sein von diesem Prinzip abzuweichen und den Zugang zur Blockchain auf bestimmte User zu begrenzen. Etliche Blockchain-Technologien bieten die Möglichkeit den Zugang zum Netzwerk zu limitieren. So ist es möglich eine eigene private Blockchain zu beginnen. Eine mit einer Zugriffskontrolle versehene Blockchain wird daher als ‚Private Blockchain‘ bezeichnet. Entsprechend ihrer Funktion im Netzwerk können manchen Teilnehmern unterschiedlich umfangreiche Rechte eingeräumt werden. So kann beispielsweise nur ein Lese-, aber kein Schreibzugriff auf die Blockchain erteilt werden. Auch der Lesezugriff kann nochmals auf die für sie relevanten Daten beschränkt werden. Nutzen mehrere Unternehmen einer Branche gemeinsam eine zugangsbeschränkte Blockchain, so wird auch von einer ‚Konsortium-Blockchain‘ gesprochen.⁴²

2.3 Schlüsselherausforderungen

Neben den vielen Möglichkeiten unterliegt der Einsatz von Blockchains noch diversen technischen sowie nicht-technischen Beschränkungen, für deren Überwindung noch Lösungsansätze gesucht werden müssen.

Die Bitcoin-Blockchain nutzt grundsätzlich ein offenes, transparentes Hauptbuch. Transaktionsdetails werden von anderen Teilnehmern vor der Bestätigung überprüft und sind für diese einsehbar. Auch wenn hinter einer Public Address ein Pseudonym steht, kann es möglich sein, die tatsächliche Identität des Teilnehmers in Erfahrung zu bringen. Diesem könnten dann sämtliche Transaktionen seines Pseudonyms zugeordnet werden, da diese in der Blockchain öffentlich einsehbar

⁴² Burgwinkel, D., Blockchaintechologie und deren Funktionsweise verstehen, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology, Berlin/Boston 2016, S.34f

sind. Dieses hohe Maß an Transparenz und fehlender Datenschutz kann in manchen Einsatzszenarien möglicherweise wiederum ein Argument gegen die Nutzung einer Blockchain sein. Einschränkungen bei Transparenz und öffentlicher Zugänglichkeit können in solchen Fällen erforderlich sein.

Da die „verwendete asymmetrische Kryptographie zu den besten und stärksten kryptographischen Methoden gehört, die es derzeit gibt“⁴³, ist eine Blockchain selbst extrem sicher vor unbefugtem Zugriff. Die größte Schwachstelle ist hier wohl der Umgang des Teilnehmers mit seinem Private Key. Er muss verhindern, dass jemand anderes diesen in Erfahrung bringen kann, darf ihn aber selbst niemals verlieren. Wie bei Schlüsseln, PINs und ähnlichem ist es auch beim Private Key. Sobald dieser, wie und warum auch immer, an eine andere Person gelangt, hat diese uneingeschränkten Zugriff auf das zugehörige Konto. Es gibt keine Zwei-Faktor-Authentifizierung, bspw. mittels eines SMS-Tan-Verfahrens, als zusätzliche Sicherheitsebene. Im Gegensatz zu den Zugangsdaten z.B. von E-Mail-Konten, besteht auch nicht die Möglichkeit einen verlorenen Private Key vom System wiederherstellen zu lassen. Der Schlüssel ist an keiner Stelle im System hinterlegt, eine Berechnung ist durch die Verwendung von Einwegfunktionen nicht möglich und es gibt keine zentrale Institution, die einen neuen Schlüssel für den Teilnehmer erstellen könnte. Ein verlorener Private Key bedeutet also gleichzeitig den Verlust des Zugriffs auf das Konto und damit auch allem, was damit verknüpft ist.

Der Einsatz von Hashpuzzles bei der Proof of Work Methode bietet zwar ein hohes Maß an Sicherheit, führt aber auch dazu, dass sich dieses System nicht auf eine beliebige Größe skalieren lässt. Die folgende Abbildung verdeutlicht den enormen Geschwindigkeitsnachteil der Bitcoin- und Ethereum-Blockchain allein im Vergleich zur Kreditkartengesellschaft VISA.

⁴³ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.218

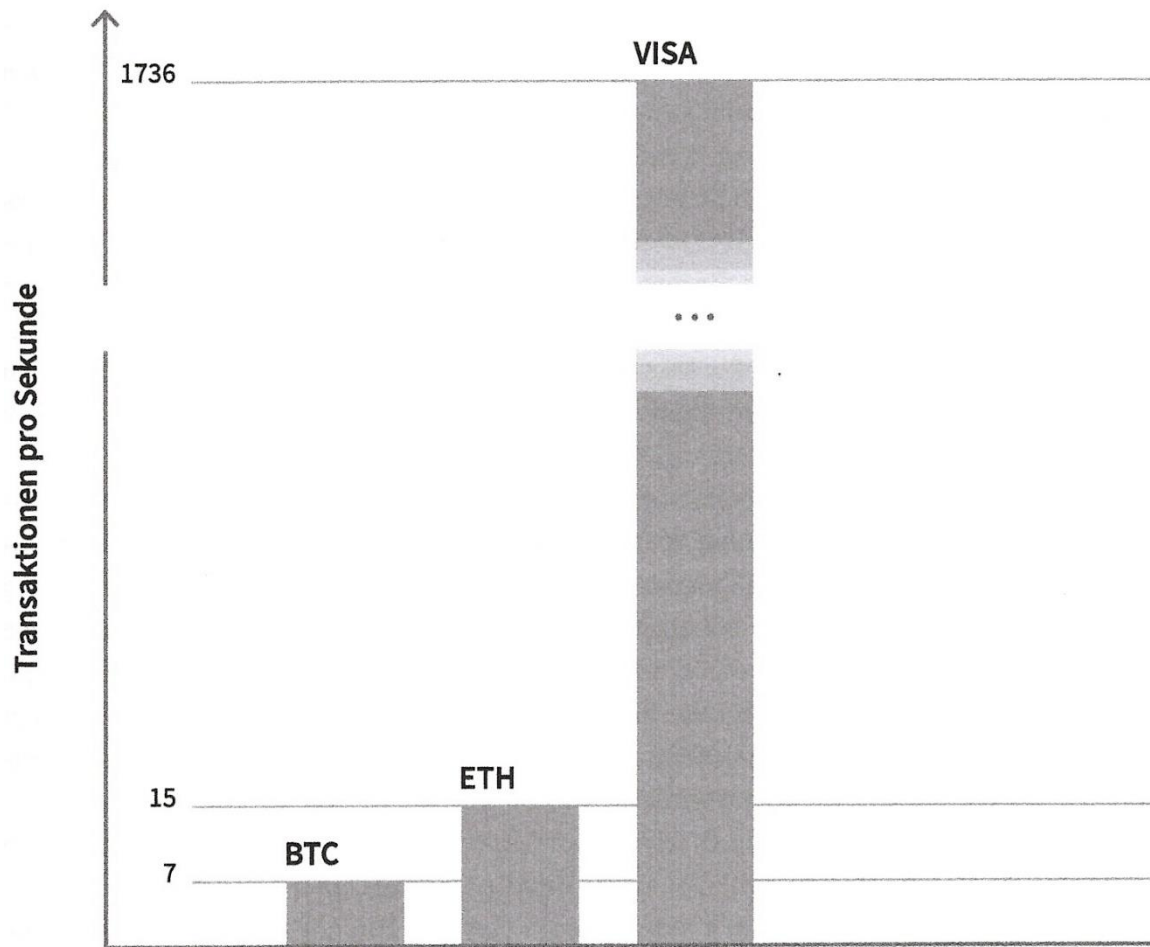


Abbildung 5 Transaktionen pro Sekunde von Bitcoin, Ethereum und VISA
 Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S.49

Eine komplette Umstellung des Zahlungsverkehrs auf nur eine oder auch mehrere, verschiedene Kryptowährungen wäre derzeit technisch überhaupt nicht verarbeitbar. Ein enormer Rückstau in der Zahlungsabwicklung wäre die Folge, was einen großflächigen, weltweiten Einsatz als Hauptzahlungsmethode derzeit nicht realisierbar macht.

Dazu kommen hohe Kosten für Hardware und Strom, um die Hashpuzzles zu lösen. Der enorme Zuwachs an Rechenleistung im Bitcoin-Netzwerk hat dazu geführt, dass sich meist nur noch teure Spezialhardware für den Miningesatz rentiert. Geben nun viele kleine Nutzer ihre Rolle als Miner auf, bildet sich im Netzwerk ein Oligopol der Rechenkapazität, das die Dezentralität des Netzwerkes gefährdet.⁴⁴

⁴⁴ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.218ff

Die *New York Times* berichtete im Juni 2016, dass sich im Bitcoin Netzwerk nur vier chinesische Unternehmen 70 Prozent des Mining-Ertrages teilen.⁴⁵ Ist im Netzwerk zu wenig Rechenleistung vorhanden, wäre aber auch das ein Risiko. Eine gewisse Mindestrechenleistung bildet gerade den Schutz vor Manipulationen durch einzelne Teilnehmer, die bspw. über sehr viel Rechenleistung verfügen. Ein Netzwerk muss also zunächst eine sogenannte kritische Größe erreichen, um ausreichend gegen 51-Prozent-Angriffe einzelner Nutzer geschützt zu sein.

Durch ihre speziellen Eigenschaften ist eine einmal entwickelte und in Betrieb genommene Blockchain außerdem nur wenig flexibel, was Veränderungen der Prozesse und Protokolle betrifft. Durch eine fehlende zentrale Instanz können diese nicht einfach erlassen, sondern müssen von einer Mehrheit der Nutzer beschlossen werden. Dabei besteht immer die Gefahr, dass sich die Blockchain aufspaltet.⁴⁶ Die Ethereum-Blockchain spaltete sich auf, nachdem sich die Community nicht einigen konnte. Aus dieser Fork genannten Spaltung gingen Ethereum (ETH) und Ethereum Classic (ETC) hervor.⁴⁷

Neben diesen technischen Beschränkungen muss zukünftig auch eine rechtliche Anerkennung sichergestellt sein. Ohne Rechtsverbindlichkeit von in der Blockchain festgehaltenen Transaktionen und Vereinbarungen wird eine Übertragung auf andere Bereiche als den netzwerkinternen Handel mit einer Kryptowährung an mangelnder Nutzerakzeptanz scheitern.⁴⁸ Die deutsche Politik hat den Handlungsbedarf bereits erkannt. Immerhin siebenmal findet sich das Wort ‚Blockchain‘ im aktuellen Koalitionsvertrag.⁴⁹ Um Akzeptanz und Vertrauen in die Technik zu fördern, muss möglichen Nutzern außerdem das Wissen um die Funktionsweise der neuen Technologie vermittelt werden, damit diese in einem gewissen Rahmen verstanden und auch angenommen wird.

Die Überwindung all dieser Herausforderungen ist von grundlegender Bedeutung, wenn die Blockchain-Technologie im Alltag Verwendung finden soll. Auf technischer

⁴⁵ Popper, N., How China Took Center Stage in Bitcoin's Civil War, in: www.nytimes.com (abgerufen am 25.09.2018)

⁴⁶ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.220f

⁴⁷ Hosp, J., Kryptowährungen, München 2018, S.112

⁴⁸ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.221

⁴⁹ CDU/CSU und SPD, Koalitionsvertrag zwischen CDU, CSU und SPD 19. Legislaturperiode, Berlin 2018, S.41ff

Seite sorgen bereits permanente Weiterentwicklung und Anpassung existierender Blockchain-Protokolle zu einer stetigen Verbesserung der Technologie. Ebenso wird die zur Verfügung stehende Hardware immer leistungsfähiger, sodass immer mehr Speicherplatz und Rechenkapazität zur Verfügung stehen. Der Erfolg von Internet und E-Commerce zeigt, dass auch die nichttechnischen Probleme gelöst werden können. Diese noch vergleichsweise jungen Technologien haben eine breite Akzeptanz und Verbreitung bei den Verbrauchern erreicht und gehören für die meisten Menschen zum Alltag.⁵⁰

⁵⁰ Drescher, D., Blockchain Grundlagen, Frechen 2017, S.221f

3 Anwendungsbereich Logistik

Einige der zuvor genannten Einsatzszenarien können sich bereits auf die Geschäftsprozesse in der Logistik auswirken. In diesem Kapitel gehe ich jedoch auf Einsatzmöglichkeiten ein, die speziell und explizit die Logistik betreffen.

3.1 Erhöhung der Transparenz entlang der Supply Chain

Der Logistikdienstleister *Hermes* führte im Jahr 2017 unter rund 200 Logistikentscheidern eine Umfrage durch. Fast die Hälfte der Befragten gab an, dass mehr Informationen von ihnen gefordert werden. „Acht von zehn deutschen Unternehmen möchten ihre Lieferkette daher transparenter gestalten.“⁵¹ Die Unternehmen erhoffen sich dadurch vor allem kürzere Reaktionszeiten bei Störungen, eine höhere Lieferqualität und effizientere Betriebsabläufe. Trotz dieser Vorteile bieten bisher nur 20% der Unternehmen eine digitale Supply Chain in Echtzeit an.⁵²

Da Transparenz eine der Haupteigenschaften einer Blockchain ist, scheint diese Technologie wie prädestiniert, um die gewünschte Transparenz auch entlang der Supply Chain zu erreichen.

Einen speziellen Anwendungsfall erprobt die Diamantenindustrie. Mithilfe der Blockchain soll unter anderem der Handel mit den sogenannten Blutdiamanten unterbunden werden. Die Firma *Everledger* aus London „hat bereits 1,6 Millionen Diamanten auf einer Blockchain registriert.“⁵³ Eigenschaften der Diamanten wie „Farbe, Karat und Zertifikatsnummer“⁵⁴ werden digital und unfälschbar gespeichert. Aktuell konzentriert sich das Angebot noch auf die Industrie, Ziel ist aber die komplette Historie der einzelnen Diamanten bis zum Endkunden transparent zu machen und diesem zur Verfügung zu stellen. So kann der Kunde bspw. vor einem

⁵¹ Hermes Team, Transparenz in der Supply Chain, in: <https://newsroom.hermesworld.com> (abgerufen am: 10.09.2018)

⁵² Ebd.

⁵³ Capital-Redaktion, Was die Blockchain für den Diamantenhandel bedeutet, in: <https://www.capital.de> (abgerufen am 14.09.2018)

⁵⁴ Ebd.

Kauf selbst die Informationen auf der Blockchain mit dem ihm zum Kauf angebotenen Stein überprüfen und die Übereinstimmung verifizieren.⁵⁵

Die Idee Rückverfolgbarkeit und Transparenz im Lebensmittelhandel zu verbessern skaliert diese Transparenz in eine deutlich größere Dimension. Dort soll jede Lieferung eine Chargennummer erhalten, welche auf der Blockchain eingetragen wird. Bei Verkauf vom Erzeuger an Händler, Lieferanten und verarbeitende Betriebe wird dieser Verlauf ebenfalls auf der Blockchain festgehalten. So kann die Herkunft der Waren eindeutig und ohne nachträgliche Manipulationen von Überwachungsstellen und auch den Konsumenten zurückverfolgt werden. Würden bei einem Erzeuger Mängel festgestellt, könnten alle betroffenen Produkte ermittelt und ein entsprechender Rückruf eingeleitet werden. Verschweigen und Verfälschen von Unterlagen wäre nicht möglich. Der Konsument könnte ebenso überprüfen, ob die Produkte tatsächlich regionalen Ursprungs sind oder alle Zutaten von einem Bio-Betrieb stammen. Betriebsgeheimnisse und Details der Kaufverträge wie z.B. Preise sind jedoch mit einem entsprechenden Zugriffsschutz zu versehen und nur für bestimmte Teilnehmer einsehbar.⁵⁶

3.2 Automatisierung von Zahlungsprozessen

Die in Abschnitt 2.2.4 vorgestellten Smart Contracts ermöglichen eine weitgehende Automatisierung verschiedener Vorgänge wie Transaktionen auf der Blockchain. Diese Anwendungs- und Automatisierungsmöglichkeiten vervielfachen sich, je mehr Daten erfasst werden. Dabei kann selbst eine manuelle Erfassung und Eingabe der Daten überflüssig werden. Die Entwicklung zum Internet der Dinge, bei dem immer mehr Gegenstände vernetzt und an das Internet angebunden werden, kann hier einen entscheidenden Beitrag leisten.

Würde man die LKWs aus dem zuvor gegebenen Beispiel mit GPS-Empfängern und einer Internetverbindung ausstatten, so könnten diese ihre Laufleistung

⁵⁵ Capital-Redaktion, Was die Blockchain für den Diamantenhandel bedeutet, in: <https://www.capital.de> (abgerufen am 26.09.2018)

⁵⁶ Merz, M., Einsatzpotenziale der Blockchain im Energiehandel, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology, Berlin/Boston 2016, S.59

selbstständig übermitteln und die Leasingrate automatisch abrechnen. Versicherungen könnten ferner aus den Daten auf das Fahrverhalten schließen und über angepasste Versicherungsbeiträge vorausschauendes und risikoarmes Fahren belohnen.⁵⁷ Mit RFID-Technik ausgestattete Container oder Ladungsträger wie Paletten würden automatisch beim Umschlag erfasst werden können. Wird bspw. ein Container auf ein Schiff geladen, wird dies automatisch von Scannern registriert und in der Blockchain erfasst. Diese Eingabe löst dann eine Zahlung der Umschlagsgebühren an den Terminalbetreiber gemäß der im Smart Contract vereinbarten Incoterms aus.

Wie weit sich diese Automatisierung realisieren lässt, hängt davon ab, welche Teilnehmer über die Blockchain miteinander verbunden sind und welche Daten erfasst werden. Ob sich jede machbare Umsetzung aber auch rentiert, muss jeweils individuell überprüft werden.

3.3 Praxisbeispiele

Ob die Blockchain-Technologie den enormen Erwartungen auch abseits der Theorie gerecht werden kann, muss sie erst noch im Tagesgeschäft beweisen. Auf zwei Feldversuche, in denen dieser Einsatz im logistischen Bereich erprobt wird, gehe ich im Folgenden ein.

3.3.1 IBM & Maersk

Das US-amerikanische IT-Unternehmen *IBM* und die weltgrößte Containerschiff-Reederei *Maersk* aus Dänemark gaben im März 2017 in einer Pressemitteilung bekannt, zusammen eine „branchenweite und grenzüberschreitende Supply Chain-Lösung auf Basis von Blockchain“ entwickeln zu wollen.⁵⁸ Als Basis dafür dient Hyperledger, eine Blockchain-Technologie, welche von *The Linux Foundation* entwickelt wurde. Hyperledger ist eine Open-Source-Initiative, d.h. der Quellcode der Software ist öffentlich einsehbar. Jeder kann den Code lesen und so seine

⁵⁷ Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S98f

⁵⁸ Kress, W., Maersk und IBM kündigen Supply-Chain-Lösung auf Blockchain-Technologie an, in: www.ibm.com (abgerufen am 26.09.2018)

Funktionsweise nachvollziehen. Ebenso kann jeder den Code ändern, optimieren und ergänzen, um ihn so für die Nutzung in bestimmten Anwendungsszenarien anzupassen.⁵⁹ Im Rahmen eines Hackathons, einer kollaborativen Software-Entwicklungsveranstaltung, entwickelte und präsentierte *IBM* das Framework Hyperledger Fabric⁶⁰. Dieses Softwaregerüst optimiert die Nutzung der Hyperledger-Blockchain für Unternehmen. Folgende Merkmale und Eigenschaften definieren die Hyperledger-Blockchain und unterscheiden sie von anderen Blockchains:

- Im Gegensatz zu bspw. der öffentlich und frei zugänglichen Bitcoin-Blockchain ist hier auch eine Zugangsbeschränkung vorgesehen. Diese wird jedoch nicht von einer zentralen Instanz festgelegt. Stattdessen gibt es „gemeinsam definierte Mitgliedschafts- und Zugriffsrechte“⁶¹. Dadurch bleibt der dezentrale Charakter des Netzwerkes gewahrt. „Neben den geschlossenen Nutzerkreisen sind aber auch öffentliche und hybride Modelle möglich.“⁶² Ein Teil der Informationen zu den Transaktionen könnte öffentlich für Verbraucher zugänglich sein, während andere Informationen für diese verschlüsselt bleiben. So könnten zwar Verbraucher z.B. den Ursprung von Produkten nachvollziehen, Details wie der Verkaufspreis bleiben jedoch Käufer und Verkäufer vorbehalten. Ebenso erhalten andere am Geschäft beteiligte Personen und Firmen nur Zugriff auf die Informationen, die sie zur Abwicklung benötigen.⁶³
- Ein Zugriff auf externe Softwareschnittstellen „oder Webservices aus den Geschäftstransaktionen“⁶⁴ ist ebenfalls möglich.
- Außerdem wurde die Hyperledger-Blockchain skalierbar entwickelt, so dass tausende Transaktionen pro Sekunde verarbeitet werden können.⁶⁵

⁵⁹ Dudenredaktion, Open-Source-Software, in: www.duden.de (abgerufen am 26.09.2018)

⁶⁰ The Linux Foundation, Hyperledger Fabric, in: www.hyperledger.org (abgerufen am 12.09.2018)

⁶¹ IBM, Hyperledger, in: www.ibm.com (abgerufen am 21.09.2018)

⁶² Ploom, T., Blockchains - wichtige Fragen aus IT-Sicht, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology, Berlin/Boston 2016, S.134

⁶³ Hyperledger, Hyperledger Fabric Explainer, in: www.youtube.com (abgerufen am 26.09.2018)

⁶⁴ Ploom, T., Blockchains - wichtige Fragen aus IT-Sicht, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology, Berlin/Boston 2016, S.134

⁶⁵ Ebd. S.133f

- Hyperledger erlaubt außerdem die Programmierung von Smart Contracts, welche hier als Chaincode bezeichnet werden. Eine Automatisierung von Geschäftsprozessen zwischen den Teilnehmern wird so ermöglicht.
- Für den Betrieb der Hyperledger-Blockchain ist keine Kryptowährung erforderlich. Ebenso entfällt kostenintensives Mining zur Schaffung von Konsens.
- Als Konsensmethode wurde keine der bisher in dieser Arbeit vorgestellten Varianten, sondern PBFT gewählt.⁶⁶ PBFT steht für Practical Byzantine Fault Tolerance und basiert auf dem Problem der byzantinischen Generäle bzw. dem byzantinischen Fehler. Auch wenn in einem Netzwerk einige Signale fehlerhaft oder manipuliert sind, kann das Netzwerk dennoch weiterarbeiten und funktionieren. Über den Konsensus stimmen gleichberechtigte, validierte Teilnehmer des Netzwerkes ab. So lange wenigstens „mehr als dreimal so viele validierte Teilnehmer in einem Netzwerk korrekt arbeiten“⁶⁷, arbeitet auch das Netzwerk korrekt und der erzielte Konsensus ist nicht manipuliert.⁶⁸ Durch die Zugangsbeschränkung der Hyperledger-Blockchain ist eine Validierung der Teilnehmer gegeben und ihre Identität ist bekannt. Den Teilnehmern kann also ein deutlich größeres Vertrauen entgegengebracht werden als in einem öffentlichen Blockchain-Netzwerk. Die Reduzierung der Angriffshürde auf weniger als die bei anderen Verfahren nötigen 51% kann in dieser Umgebung noch als sicher angenommen werden. Durch die Zugangsbeschränkung wird auch eine mögliche Sybill-Attacke verhindert. Bei dieser würde ein Teilnehmer viele neue Miner erstellen und diese in seinem Sinne abstimmen lassen.⁶⁹ Da neue Teilnehmer jedoch zunächst überprüft werden, bevor sie vollen Zugang zum Netzwerk erhalten, wäre ein solcher Angriff sehr aufwendig und unterm Strich vermutlich wirtschaftlich unrentabel. Schließlich müsste für jeden Teilnehmer eine gefälschte Identität erstellt werden, unter der dieser dann in das Netzwerk aufgenommen wird.

⁶⁶ IBM, Hyperledger, in: www.ibm.com (abgerufen am 21.09.2018)

⁶⁷ Metzger, J., Konsensmechanismus, in: <https://wirtschaftslexikon.gabler.de> (abgerufen am 26.09.2018)

⁶⁸ Ebd.

⁶⁹ Hosp, J., Kryptowährungen, München 2018, S.64

Die Unterschiede zu den Blockchains von Bitcoin und Ethereum werden in der folgenden Tabelle noch einmal veranschaulicht.

	Bitcoin	Ethereum	Hyperledger Fabric
Kryptowährung erforderlich	Bitcoin	Ether, benutzererstellte Kryptowährungen	Keine
Netz	Öffentlich	Öffentlich oder mit Berechtigung	Mit Berechtigung
Transaktionen	Anonym	Anonym oder nicht öffentlich	Öffentlich oder vertraulich
Konsens	Ausführungsnachweis	Ausführungsnachweis	PBFT
Smart Contracts	Keine	Ja	Ja (Chaincode)
Programmiersprache	C++	Golang, C++, Python	Golang, Java

*Tabelle 1 Unterschiede der Blockchains von Bitcoin, Ethereum und Hyperledger Fabric
eigenes Werk in Anlehnung an: IBM, Hyperledger, in: www.ibm.com (abgerufen am 21.09.2018)*

Auf dieser Grundlage soll die gesamte Supply Chain nun digitalisiert werden. Der Blockchain kommt dabei zukünftig die Aufgabe zu, die vielen unterschiedlichen und untereinander nicht kompatiblen Softwaresysteme der verschiedenen Teilnehmer zu überbrücken. Dadurch würde es keinen Medienbruch durch Nutzung von bspw. Fax oder E-Mail-Anhängen mehr geben, da die mehrfache Digitalisierung der gleichen Daten per Hand, also das Abtippen ausgedruckter oder per E-Mail versandter Dokumente in das jeweils genutzte System der Teilnehmer, entfällt. Ebenso wird ein teurer Kurierversand, bspw. von originalen Konnossementen, überflüssig, da diese Wertpapiere bei Nutzung einer Blockchain nicht mehr physisch benötigt werden. Alle Dokumente und Papiere sollen über das Netzwerk digital zwischen Spediteuren, Reedereien, Häfen und Zollbehörden ausgetauscht werden. Das mögliche Einsparungspotenzial zeigt sich an den Zahlen, die *Maersk* für die Versendung eines einzigen Kühlcontainers aus Ostafrika nach Europa angibt. Zurzeit führen dafür fast 30 Personen und Organisationen über 200 Interaktionen untereinander aus.⁷⁰ Durch die Digitalisierung sollen diese Prozesse deutlich

⁷⁰ Kress, W., Maersk und IBM kündigen Supply-Chain-Lösung auf Blockchain-Technologie an, in: www.ibm.com (abgerufen am 12.09.2018)

vereinfacht, teilweise automatisiert und Verzögerungen bei der Übertragung minimiert werden.

In einem Beispielvideo zeigen *IBM* und *Maersk*, wie die zugehörige Dokumentenabwicklung bei Nutzung einer Blockchain aussehen soll.

Zunächst erstellt der Exporteur eine Liste der Waren, die versendet werden sollen. Mit dem Absenden an alle Beteiligten entsteht daraus ein Smart Contract. Die Export-Behörden können in diesem die nötigen Freigaben für die Waren erteilen. Containernummer und Aufnahme durch den Vorlaufspediteur werden ebenfalls eingetragen und so an den Exporthafen avisiert. Dabei können alle auf der Blockchain eingetragenen Informationen von den Beteiligten jederzeit abgerufen werden. Zudem lässt sich lückenlos nachvollziehen, wer wann etwas eingetragen oder freigegeben hat und wie der Container bewegt wurde. Im Empfangshafen kann von den lokalen Behörden direkt auf die Informationen und Dokumente zugegriffen werden, welche vom Versender und den Behörden im Herkunftsland eingetragen wurden. Sobald die Bedingungen im Smart Contract erfüllt wurden, geben die ebenfalls beteiligten Banken von Käufer und Verkäufer automatisch die vereinbarte Zahlung frei.⁷¹

Anfang des Jahres 2018 gaben die beiden Unternehmen die Bildung eines Joint-Ventures bekannt. *Maersk* und *IBM* wollen so ihre Lösungen an mehr Unternehmen weltweit vermarkten und ihre Plattform etablieren. Zwei Kernfähigkeiten werden für die Plattform angegeben:

- Zum einen „eine End-to-End-Sichtbarkeit der Supply Chain“⁷², also Zugriff aller Beteiligten auf alle Informationen und Lieferereignisse entlang der gesamten Supply Chain in Echtzeit.
- Zum anderen soll über blockchainbasierte Smart Contracts ein papierloser Handel ermöglicht werden. Alle Dokumente werden digital erstellt und sicher

⁷¹ IBMBlockchain, IBM and Maersk demo: Cross-border supply chain solution on blockchain, in: [www.youtube.com](https://www.youtube.com/watch?v=...) (abgerufen am 26.09.2018)

⁷² IBM, Maersk und IBM bilden Joint Venture für Blockchain, in: [https://www.ibm.com](https://www.ibm.com/press/...) (abgerufen am 26.09.2018)

zwischen den Beteiligten ausgetauscht. Arbeits- und Kostenaufwand sowie Fehlerquellen werden durch die automatische Bearbeitung reduziert.

Neben Firmen wie *General Motors* und *Procter and Gamble* und den Zollbehörden von Singapur und Peru haben auch „die globalen Terminalbetreiber *APM Terminals* und *PSA International*“⁷³ Interesse an der Plattform.⁷⁴

Im August 2018 stellten die beiden Unternehmen schließlich die gemeinsam entwickelte Plattform **TradeLens** als Ergebnis ihrer Zusammenarbeit vor. 94 Teilnehmer, darunter „Spediteure, Häfen, Zollbehörden, Banken, Logistikdienstleister und Unternehmen“⁷⁵ aus der ganzen Welt haben sich zur Teilnahme an der Plattform entschlossen. Neben *Maersk* beteiligen sich unter anderem auch die Reedereien *Hamburg Süd* und *Pacific International Lines (PIL)*, die Zollbehörden aus den Niederlanden, Singapur und Australien sowie die Logistikunternehmen *Agility* und *Damco*. Die Teilnehmer haben bereits über 150 Millionen Versandvorgänge im System erfasst und derzeit kommen täglich eine Million weitere hinzu. Die bisherige Erprobung wird bereits als Erfolg bewertet. Für einzelne Sendungen konnte die Transitzeit um 40% gesenkt und damit tausende Dollar gespart werden. Ebenso wird „die Standardisierung und damit die Vereinfachung und Verschlinkung des Informationsaustauschs“⁷⁶ positiv hervorgehoben. Das Weltwirtschaftsforum schätzt zudem das Wachstumspotential für den Welthandel auf fast 15%, wenn die aktuell bestehenden Barrieren beseitigt werden sollten.⁷⁷ Durch die Beteiligung von *Maersk* und den damit verbundenen Fokus auf Seeverkehre, könnte TradeLens entscheidend dazu beitragen, da „90% aller globalen Güter als Seefracht befördert“⁷⁸ werden. Nachdem die Plattform

⁷³ IBM, Maersk und IBM bilden Joint Venture für Blockchain, in: <https://www.ibm.com> (abgerufen am 26.09.2018)

⁷⁴ Ebd.

⁷⁵ Ostler, U., Tradelens von Maersk und IBM soll das Schifffahrtsökosystem umkempeln (sic), in: www.datacenter-insider.de (abgerufen am 26.09.2018)

⁷⁶ Ebd.

⁷⁷ Ebd.

⁷⁸ Kress, W., Maersk und IBM kündigen Supply-Chain-Lösung auf Blockchain-Technologie an, in: www.ibm.com (abgerufen am 26.09.2018)

aktuell nur für die Erstanwender zugänglich ist, soll diese am Ende des Jahres in vollem Umfang für weitere Teilnehmer geöffnet werden.⁷⁹

3.3.2 GS1

Der Dienstleister GS1 hat sich darauf spezialisiert die Prozesse verschiedener Marktteilnehmer zu optimieren und aufeinander abzustimmen. Das Unternehmen „begleitet die Entwicklung und Implementierung offener, branchenübergreifender, weltweit gültiger Standards.“⁸⁰ Die entwickelten Standards sollen helfen komplexe Waren- und Informationsströme zu vereinfachen und auch zu automatisieren.⁸¹ Ein solcher Standard ist bspw. die Globale Lokationsnummer (GLN), die genutzt wird, um Unternehmen und deren Standorte eindeutig zu bezeichnen. Über die 13-stellige Nummer können eindeutige Firmennamen und Adressen angerufen werden. Fehlinformationen durch unklare Schreibweisen werden so vermieden.⁸²

Da der Blockchain-Technologie in Zukunft eine bedeutende Rolle zugeschrieben wird, und sie die Grundlage für neue Standards bilden könnte, hat GS1 sich zu einem Pilotprojekt entschlossen. Die theoretischen Potenziale der Blockchain sollen dabei beim Einsatz im Tagesgeschäft überprüft werden und nicht in einer isolierten Testumgebung.⁸³ Im Rahmen des diesjährigen Feldversuchs sollen vor allem allgemeine Erkenntnisse gewonnen werden, wie leistungsfähig und flexibel die Blockchain-Technologie eingesetzt werden kann. Gleichzeitig soll das Erreichte aber auch Erkenntnisse über einen möglicherweise konkreten praktischen Nutzen liefern.⁸⁴

Als konkreten Anwendungsfall für das Pilotprojekt hat GS1 sich daher für den Ladungsträgertausch, genauer den Palettenschein, entschieden. Dieser kommt immer dann zum Einsatz, wenn eine Lieferung auf Ladungsträgern erfolgt, der

⁷⁹ Moneycab, IBM und Maersk führen Blockchain-Lösung TradeLens für Lieferkette ein, in: www.moneycab.com (abgerufen am 26.09.2018)

⁸⁰ GS1 Germany, Über uns, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁸¹ Ebd.

⁸² GS1 Germany, Unternehmen mit der GLN identifizieren, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁸³ Haas-Hamann, R., Palettentrauma adé?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁸⁴ GS1 Germany, Wenn Hype auf Wirklichkeit trifft: GS1 Germany startet Blockchain-Piloten, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Empfänger jedoch kein Leergut zum Tausch bereitstellen kann. Auf dem Schein werden „Anzahl, Art und Güte der Ladungsträger“⁸⁵ dokumentiert. Zu einem späteren Zeitpunkt kann der Palettenschein gegen die aufgeführten Ladungsmittel eingetauscht werden. Dadurch fungiert er als ein Wertpapier. Bis heute existiert für den Palettenschein kein digitales System. Stattdessen erfolgt die Dokumentation fast ausschließlich manuell und auf Papier. Betrachtet man die zugehörigen Zahlen, wird das riesige Ausmaß des Optimierungspotenzials deutlich. „Über 500 Mio. Europaletten im Wert von mindestens 2,5 Mrd. Euro“⁸⁶ befinden sich in Europa im Umlauf. Mehr als 150 Mio. jährliche Tauschvorgänge führen zu über 300 Mio. manuellen Dokumentationen, da beide am Tausch beteiligten Parteien diesen für sich dokumentieren.⁸⁷

Am 18.04.2018 fiel der Startschuss für das Pilotprojekt, das GS1 gemeinsam mit etwa 20 weiteren Unternehmen durchführt. Darunter sind viele bekannte Firmen aus verschiedenen Branchen. Unter anderem beteiligen sich aus dem Handel *dm-drogerie markt* und *Kaufland*, aus der Industrie *Beiersdorf* und *Dr. Oetker* und aus der Logistikbranche *Deutsche Bahn* und *Nagel-Group*. Beratend ist das *Fraunhofer-Institut für Angewandte Informationstechnik FIT* involviert. Der Anbieter von Unternehmenssoftware *SAP* ist Technologiegeber und für die technische Umsetzung verantwortlich. Die Teilnehmer haben großes Interesse an dem Thema Blockchain und erhoffen sich, während der Erprobung belastbare Erkenntnisse über diese Technik zu sammeln. Abseits des Erkenntnisgewinns wäre eine tatsächliche Optimierung des Lademitteltauschs ein Quantensprung.⁸⁸

In diversen Workshops ermittelten Vertreter aus den beteiligten Unternehmen welche gemeinsamen Anforderungen sie an die Anwendung haben. Anhand dieser wird eine kompatible Plattform ausgewählt und die Softwareentwicklung begonnen.⁸⁹

⁸⁵ Haas-Hamann, R., Palettenchaos adé?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁸⁶ Ebd.

⁸⁷ Ebd.

⁸⁸ GS1 Germany, Beendet Blockchain die Zettelwirtschaft?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁸⁹ Stettiner, E., Projektteam blickt auf Nutzer, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Bei der Wahl der zu nutzenden Blockchain-Technologie fiel die Wahl auf das Multichain-Protokoll. „Im Vergleich zu einigen anderen Blockchain-Technologien bietet es insbesondere eine geringe Komplexität, niedrige Betriebskosten, eine hohe Leistungsfähigkeit [...] sowie die Möglichkeit, sie möglichst einfach über verschiedene Infrastrukturen zu verteilen.“⁹⁰ Die genutzte Blockchain ist privat und mit einer Zugangsbeschränkung versehen (Private Permissioned Blockchain), Lese- und Schreibzugriff ist also auf bestimmte, bekannte Teilnehmer beschränkt. Da mehrere Unternehmen beteiligt sind, trifft auch die Bezeichnung Konsortium-Blockchain zu. Die Teilnehmer während des Pilotprojekts kennen einander und auch im späteren Betrieb sollen sich alle Teilnehmer untereinander kennen und eindeutig identifizieren können. Gemeinsam wurden daher Kriterien für „die Aufnahme und Zusammenarbeit mit weiteren Teilnehmern“⁹¹ festgelegt. Da die digitale Erfassung der Daten über eine Applikation erfolgt „die sowohl von Smartphones und Tablets als auch vom Desktop-PC zu nutzen ist“⁹², können alle involvierten Personen wie Fahrer, Lager- und Büromitarbeiter damit gleichermaßen auf die Blockchain zugreifen und Daten auf dieser hinterlegen. Bei der entwickelten Nutzeroberfläche wurde besonders Wert auf eine intuitive Bedienbarkeit durch die Anwender geachtet. Die auf der nächsten Seite folgende Abbildung zeigt einen Screenshot aus einem frühen Prototypen der entwickelten Smartphone-App.

⁹⁰ Uhde, T., Das Palettenchaos auf die Kette kriegen: Die Systemarchitektur zum Pilotprojekt, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁹¹ Ebd.

⁹² Ebd.

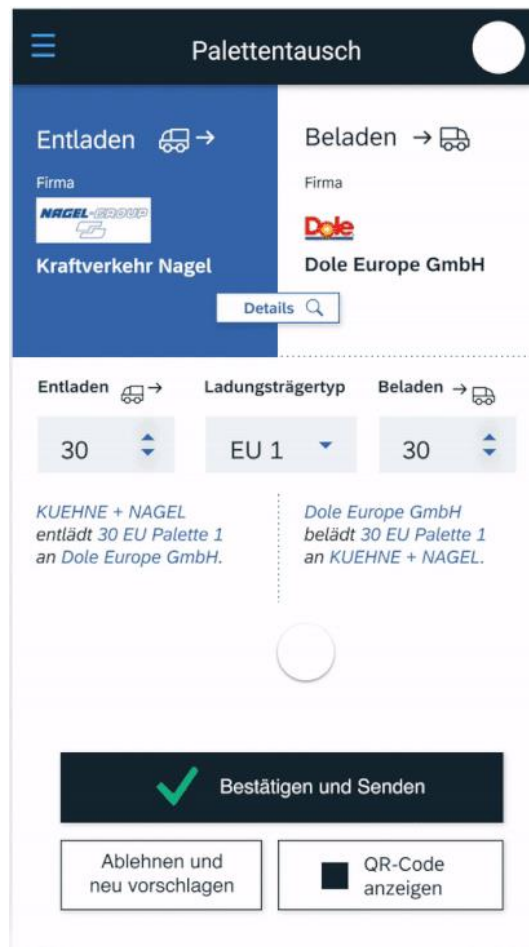


Abbildung 6 Screenshot der Smartphone-App

Mohr, O., User Centered Design: Die Palettentausch-App wird getestet, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Durch die klare Gestaltung sollen fehlerhafte Eingaben durch die Nutzer möglichst vermieden werden, da nachträgliche Änderungen und Korrekturen bei Verwendung einer Blockchain nur mit viel Aufwand erfolgen könnten, weil sie die Zustimmung aller Beteiligten sowie einen erneuten Verifizierungsprozess erfordern. Die Übertragung der erfassten Daten auf die Blockchain erfolgt automatisch „entweder über die SAP Cloud Platform Blockchain oder alternativ über einen eigenen Zugangspunkt des jeweiligen Teilnehmers“⁹³ Die SAP Cloud Platform Blockchain stellt Knoten für die Teilnehmer zur Verfügung, ebenso haben die Teilnehmer aber auch die Möglichkeit einen eigenen, externen Knoten zu betreiben und damit zur Dezentralisierung des Netzwerkes beizutragen. Keiner der Teilnehmer verfügt

⁹³ Uhde, T., Das Palettenchaos auf die Kette kriegen: Die Systemarchitektur zum Pilotprojekt, in: www.gs1-germany.de (abgerufen am 26.09.2018)

dadurch über die alleinige Datenhoheit. Weiterhin von Vorteil ist, dass die Teilnehmer die Möglichkeit haben individuelle und bestehende Software über Schnittstellen an das Netzwerk anzubinden.⁹⁴

Diverse Standards, die GS1 bereits entwickelt und etabliert hat, können in dem Projekt genutzt werden, wie zum Beispiel die von GS1 entwickelten GLNs zur eindeutigen Identifizierung der Tauschpartner. Durch diese Etablierung und Verwendung in bestehenden Geschäftsprozessen vieler Unternehmen wird die Einbindung der Blockchain bei den Teilnehmern erleichtert.⁹⁵

Nach der umfangreichen Entwicklung von Anforderungen, Software und Systemarchitektur steht im nächsten Schritt der Praxistest bevor, welcher für die zweite Oktoberhälfte terminiert wurde. Einige der beteiligten Unternehmen aus verschiedenen Branchen werden dann zwei Wochen lang alle Tauschvorgänge von Lademitteln in der Anwendung erfassen und dokumentieren. Zusätzlich erfolgt parallel weiterhin die Erfassung und Verarbeitung in den jeweiligen etablierten Systemen. Der praxisnahe Testbetrieb soll durch die Verwendung von echten Daten aus dem Tagesgeschäft möglichst belastbare Ergebnisse liefern. Insgesamt sollen während des Feldversuchs über 2.000 Einträge über Lademitteltausche an den verschiedenen Schnittstellen erstellt werden.⁹⁶

Im Anschluss an die Testphase folgt die Auswertung der gesammelten Daten und erste Handlungsempfehlungen für die Praxis müssen entwickelt werden. Diese Ergebnisse sollen schließlich am 6. Dezember der Öffentlichkeit präsentiert und auch zugänglich gemacht werden.⁹⁷

⁹⁴ Uhde, T., Das Palettenchaos auf die Kette kriegen: Die Systemarchitektur zum Pilotprojekt, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁹⁵ Träger, R., Was haben (GS1) Standards mit Blockchain zu tun?, in: www.gs1-germany.de (abgerufen am: 26.09.2018)

⁹⁶ Wunsch, A., Der Praxistest – Wir gehen auf Ganze!, in: www.gs1-germany.de (abgerufen am: 26.09.2018)

⁹⁷ Haas-Hamann, R., Palettenchaos adé?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

4 Schritte zur Blockchain – Implementierung

Der Handel mit unterschiedlichen Kryptowährungen ist für jeden mit Internetzugang nach kurzer Einarbeitung recht einfach möglich, aber in anderen Bereichen kann eine Blockchain noch nicht problemlos genutzt werden. Zwar existieren bereits diverse Blockchain-Technologien und inzwischen auch diverse zugehörige Software, einfache Plug and Play Lösungen, die nur noch installiert werden müssen, gibt es bisher jedoch nicht. Eine Implementierung geht daher derzeit immer auch mit einer umfangreichen Entwicklungsphase einher, weil die vorhandenen Blockchain-Systeme jeweils individuell auf den konkreten Anwendungsfall hin angepasst werden müssen. Um ein bestehendes System auf die Verwendung der Blockchain-Technologie umzustellen oder völlig mit dieser zu ersetzen, sind daher vorab viele Planungen erforderlich.⁹⁸

Grundsätzlich ist zu prüfen, ob eine Blockchain überhaupt aus technologischer Sicht die beste Wahl ist und diese einen entscheidenden Mehrwert bietet. Es gibt schließlich eine Menge anderer Datenbanksysteme, welche technisch weit entwickelt, praxiserprobt und relativ einfach zu implementieren sind.⁹⁹ Der dezentrale und unabhängige Aufbau einer Datenbank ohne zentrale Kontrollinstanz bei gleichzeitiger Sicherheit und Unverfälschbarkeit der gespeicherten Daten ist aber die große Stärke von Blockchains. Dieses dezentrale Konzept als rein private Blockchain zentral in einem Unternehmen aufzusetzen und zu kontrollieren, macht diesen Vorteil zunichte. Wird eine gewisse unternehmensübergreifende Transparenz und Zusammenarbeit von vornherein ausgeschlossen, ist eine Blockchain daher nicht die richtige Wahl. Eine Kontrolle durch bspw. Administratoren ist nicht vorgesehen und lässt sich, wenn gewünscht, mit herkömmlichen zentralen Datenbanken besser und effizienter realisieren.¹⁰⁰ Fällt die Entscheidung schließlich auf eine blockchainbasierte Lösung, so sind Anforderungen an die Anwendung zu sammeln und zu formulieren. Neben der Technologie muss aber auch das Unternehmensumfeld betrachtet werden, in

⁹⁸ Hardt, H., Blockchain ist kein Plug'n'Play, in: www.gs1-germany.de (abgerufen am 26.09.2018)

⁹⁹ Haas-Hamann, R., Acht Praxistipps für ein erfolgreiches Blockchain-Projekt, in: www.gs1-germany.de (abgerufen am 26.09.2018)

¹⁰⁰ Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S. 74

welches diese eingeführt werden soll. Besonders das hohe Maß an Transparenz bedeutet für viele Unternehmen eine große Umstellung.¹⁰¹

Die verschiedenen Schritte, die im Entwicklungsprozess nötig sind, hat GS1 im Rahmen des Pilotprojekts zur Digitalisierung und Standardisierung des Palettenscheins ausführlich dokumentiert.¹⁰²

Nachdem der Anwendungsfall definiert wurde, müssen die Anforderungen formuliert werden. In den beiden vorgestellten Beispielen waren an der Entwicklung viele Unternehmen aus verschiedenen Branchen beteiligt. Da die fertige Anwendung von allen Teilnehmern genutzt werden soll, ist es wichtig auch alle an der Entwicklung zu beteiligen. Bei GS1 geschah dies in mehreren Workshops in denen Vertreter der Unternehmen ihre etablierten Prozesse vorstellten. Obwohl es immer um die Handhabung des Palettenscheins geht, gibt es eine große Bandbreite verschiedener Umsetzungen in den Unternehmen. Nach und nach werden daraus allgemeine Anforderungen entwickelt, in denen sich alle Teilnehmer wiederfinden.

Anhand der gesammelten Kriterien erfolgt anschließend die Auswahl einer geeigneten Plattform.¹⁰³ Neben den Möglichkeiten sind auch die Einschränkungen der verschiedenen Technologien ausschlaggebend dafür, welche Plattformen infrage kommen.¹⁰⁴

Im nächsten Schritt erfolgt die Anpassung der gewählten Plattform. Es wird ein erster Prototyp der Anwendung entwickelt und unter simulierten Bedingungen getestet.¹⁰⁵ Erste Fehler können hier bereits vor einem größeren Test im Praxisbetrieb entdeckt und behoben, ebenso kann ein erstes Feedback von Testnutzern eingeholt werden, ob die zu Beginn gestellten Anforderungen berücksichtigt und zugänglich umgesetzt wurden.¹⁰⁶ Um den Aufwand für nötige Neuentwicklungen möglichst gering zu halten, sollten bereits entwickelte und

¹⁰¹ Haas-Hamann, R., Acht Praxistipps für ein erfolgreiches Blockchain-Projekt, in: www.gs1-germany.de (abgerufen am 26.09.2018)

¹⁰² Haas-Hamann, R., Palettenchaos adé?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

¹⁰³ Stettiner, E., Projektteam blickt auf Nutzer, in: www.gs1-germany.de (abgerufen am 26.09.2018)

¹⁰⁴ Henrik, H., Blockchain ist kein Pug'n'Play, in: www.gs1-germany.de (abgerufen am 26.09.2018)

¹⁰⁵ Haas-Hamann, R., Palettenchaos adé?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

¹⁰⁶ Mohr, O., User Centered Design: Die Palettentausch-App wird getestet, in: www.gs1-germany.de (abgerufen am 26.09.2018)

etablierte Standards aufgegriffen werden. Neben den GLNs können das im logistischen Kontext bspw. Containernummern oder Incoterms sein.

Anschließend kann ein erster Praxistest erfolgen, wobei sich zeigt, ob die Theorie in der Praxis besteht und alle relevanten Faktoren bedacht wurden. Durch den Einsatz im Tagesgeschäft werden belastbare Ergebnisse unter möglichst alltäglichen Bedingungen gesammelt. Zudem wird der gesamte Test protokolliert, um im Anschluss eine umfassende Auswertung vornehmen zu können.¹⁰⁷

Diese Auswertung der gesammelten Ergebnisse schließt den Praxistest ab. Je nach Verlauf der Testphase und dem gezogenen Fazit werden auch entsprechende Handlungsempfehlungen gegeben. Diese könnten zum Beispiel konkrete Verbesserungen vorschlagen oder zu weiteren Tests raten, wodurch sich die entsprechenden Phasen wiederholen. Im schlimmsten Fall kann aber auch eine Beendigung des gesamten Projekts beschlossen werden.¹⁰⁸

Die auf der nächsten Seite folgende Abbildung fasst die einzelnen Phasen des Pilotprojektes übersichtlich zusammen.

¹⁰⁷ Wunsch, A., Der Praxistest - Wir gehen aufs Ganze!, in: www.gs1-germany.de (abgerufen am 26.09.2018)

¹⁰⁸ GS1 Germany, Wenn Hype auf Wirklichkeit trifft: GS1 Germany startet Blockchain-Piloten, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Projektverlauf in fünf Phasen:

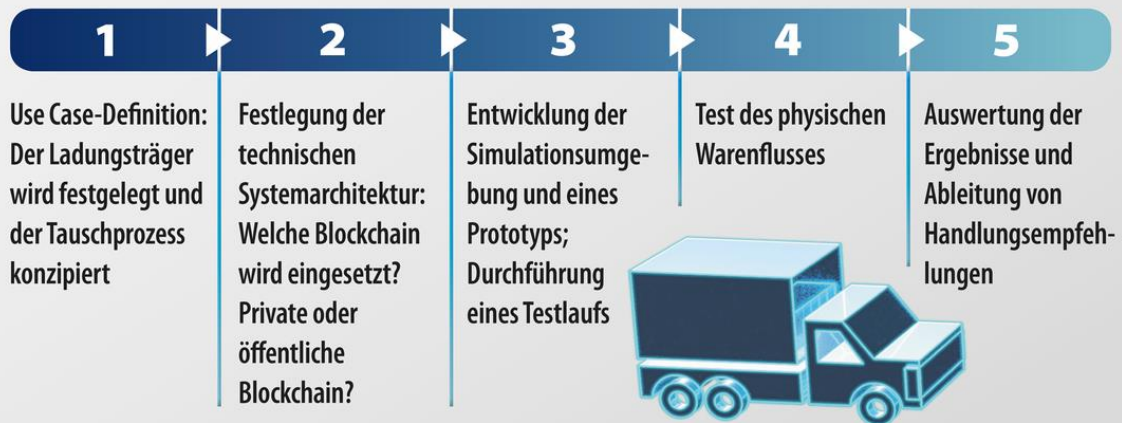


Abbildung 7 Phasen des Pilotprojektes zur Digitalisierung des Palettenscheins
 GS1 Germany, Wenn Hype auf Wirklichkeit trifft: GS1 Germany startet Blockchain-Piloten,
 in <https://www.gs1-germany.de> (abgerufen am 26.09.2018)

Rät die Handlungsempfehlung in Phase 5 zu einer Implementierung des Systems, sind eventuell die rechtlichen Rahmenbedingungen nochmals zu überprüfen. Haftungsrahmen und Verantwortlichkeiten müssen dazu ebenso geklärt sein wie die juristische Anerkennung der Daten in der Blockchain. Dies ist gerade bei internationalen Projekten oder bei der Einbindung offizieller Stellen wie z.B. Zollbehörden wichtig.

Soll ein unternehmensübergreifendes Blockchain-System implementiert werden, sind viele Fragen zu klären und Probleme zu lösen. Auf den ersten Blick scheinen diese hauptsächlich technischer Natur zu sein. Bisher fehlen noch ausgereifte Anwendungen und es hakt oftmals an einer Vernetzung der beteiligten Unternehmen. Häufig sorgt auch die Nutzung von unterschiedlichen, individuellen IT-Systemen dafür, dass Informationen nicht einfach automatisch ausgetauscht werden können, denn die Softwares verfügen über keinerlei Schnittstellen, über die sie automatisch miteinander kommunizieren könnten. Ebenso schrecken Zeit- und Kostenaufwand für die Implementierung viele Unternehmen noch ab.¹⁰⁹

¹⁰⁹ Hermes Team, Transparenz in der Supply Chain, in: <https://newsroom.hermesworld.com> (abgerufen am 26.09.2018)

Aber auch die Transparenz einer Blockchain ist für die Teilnehmer noch etwas Ungewohntes. Daten preiszugeben fällt den Unternehmen schwer, wenn jeder Teilnehmer alles sehen darf, sagt bspw. Apostolos Couvaras, Manager Corporate Network Innovation bei der *Lekkerland AG*. Auch wenn die Blockchain-Technologie immer mit Vertrauen in Verbindung gebracht wird, so fällt es doch schwer einem System ohne zentrale Instanz zu vertrauen, gerade wenn ein etabliertes System wie der Palettenschein ersetzt werden soll. Stand zunächst die technische Umsetzung und Machbarkeit im Fokus des Projekts, so stellten sich für ihn mit der Zeit mehr Fragen nach einem nötigen Kulturwandel in den Unternehmen und deren Einstellung zum Thema Digitalisierung.¹¹⁰

¹¹⁰ Couvaras, A., Governance: Im Kern geht es um Vertrauen, in: www.gs1-germany.de (abgerufen am 26.09.2018)

5 Fazit und Ausblick

Die extremen Kursgewinne und -verluste innerhalb kürzester Zeit sorgten für einen regelrechten Hype um die Kryptowährung Bitcoin. Im gleichen Zug wurde auch die zugrunde liegende Technologie, die Blockchain, bekannt. Diese ist zwar eng mit Bitcoin verbunden, bietet jedoch darüber hinaus viele weitere Potentiale und muss daher auch losgelöst von Kryptowährungen betrachtet werden. Bitcoin ist derzeit eher ein Spekulationsobjekt als ein Zahlungsmittel und wird nur in den wenigsten Fällen offiziell akzeptiert.¹¹¹ Manche Nationen erlassen sogar Verbote für den Handel mit Kryptowährungen. Prognosen zur Zukunft von Bitcoin und Kryptowährungen im Allgemeinen sind daher schwierig und fallen eher durchwachsen aus. Im Gegensatz dazu „sagen fast alle Experten der Blockchain-Technologie eine goldene Zukunft voraus.“¹¹² Die Veröffentlichung als Open-Source Software ermöglichte eine umfassende Weiterentwicklung der ursprünglichen Bitcoin-Blockchain. So entstanden neben weiteren Kryptowährungen auch neue Funktionen wie bspw. Smart Contracts. Die transparente, unmanipulierbare, dezentrale Datenbank hat in der Folge das Interesse verschiedenster Branchen geweckt. Dienstleister mit zentralisierten Servern oder Cloud-Diensten sollen umgangen und Teilnehmer des Netzwerkes direkt miteinander verbunden werden.¹¹³

Damit die Auswirkungen der Blockchain-Technologie so immens werden, wie es diverse Prognosen beschreiben, muss sie eine umfassende Etablierung erreichen. Die Initiatoren der beiden vorgestellten Beispiele versuchen dies zu erreichen, indem sie von Anfang an verschiedene Teilnehmer aus allen betroffenen Branchen und Bereichen an der Entwicklung beteiligen. Durch die Veröffentlichung der Ergebnisse im Anschluss an die Entwicklungs- und Erprobungsphase und der Öffnung des geschaffenen Netzwerkes für weitere Teilnehmer soll sichergestellt sein, dass die entwickelte Anwendung allen Teilnehmern Vorteile bietet und jedem die nötigen Funktionen zur Verfügung stehen. Zum anderen soll durch die Öffnung für weitere Teilnehmer ein möglichst großes Wachstum des Netzwerkes erreicht werden. Eine Insellösung, die sich auf einen bestimmten Teilnehmerkreis

¹¹¹ Rosenberger, P., Bitcoin und Blockchain, Berlin 2018, S.2f

¹¹² Specht, P., Die 50 wichtigsten Themen der Digitalisierung, München 2018, S. 219

¹¹³ Ebd., S.219f

beschränkt, würde wieder eine Datenübertragung per E-Mail oder ähnlichem erforderlich machen, sobald externe Unternehmen an der Logistikkette beteiligt werden. Wenn erst einmal der Großteil der Unternehmen sich einem System angeschlossen hat, stehen die Chancen jedoch gut, dass sich dieses als Standard etablieren wird.

Entscheidend für den Erfolg von blockchainbasierten Netzwerken wird sein, dass die entwickelten Anwendung den Teilnehmern klare Vorteile bieten, technisch weit genug ausgereift sind um, einen stabilen Betrieb zu gewährleisten, die rechtlichen Rahmenbedingungen auch beim internationalen Einsatz feststehen und sich dadurch viele Teilnehmer gewinnen lassen, damit das Netzwerk die nötige Größe erreicht.

Ob und wie schnell dies gelingen wird, lässt sich nur schwer sagen. Die technischen Probleme werden zunehmend beseitigt. Ein Umdenken in der Unternehmenskultur hin zu mehr Transparenz könnte teilweise noch länger dauern. Viel wird von den Ergebnissen der ersten Feldversuche abhängen, welche zum Jahresende vorliegen sollen. Sollten sich die gesteckten Erwartungen umsetzen lassen, könnte der globale Handel jedoch enorm davon profitieren.

Quellenverzeichnis

BitInfoCharts, Bitcoin Hashrate historical chart, in: <https://bitinfocharts.com>, (abgerufen am 23.09.2018)

Burgwinkel, D., Blockchaintechnologie und deren Funktionsweise verstehen, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology: Einführung für Business- und IT Manager, Berlin/Boston 2016, S.34f

Capital-Redaktion, Was die Blockchain für den Diamantenhandel bedeutet, in: www.capital.de, (abgerufen am 26.09.2018)

CDU/CSU und SPD, Koalitionsvertrag zwischen CDU, CSU und SPD 19. Legislaturperiode, Berlin 2018

Couvaras, A., Governance: Im Kern geht es um Vertrauen, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Drescher, D., Blockchain Grundlagen: Eine Einführung in die elementaren Konzepte in 25 Schritten, Frechen 2017

Dudenredaktion, Open-Source-Software, in: www.duden.de (abgerufen am 26.09.2018)

GS1 Germany, Beendet Blockchain die Zettelwirtschaft?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

GS1 Germany, Über uns, in: www.gs1-germany.de (abgerufen am 26.09.2018)

GS1 Germany, Unternehmen mit der GLN identifizieren, in: www.gs1-germany.de (abgerufen am 26.09.2018)

GS1 Germany, Wenn Hype auf Wirklichkeit trifft: GS1 Germany startet Blockchain-Piloten, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Hardt, H., Blockchain ist kein Plug'n'Play, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Haas-Hamannt, R., Acht Praxistipps für ein erfolgreiches Blockchain-Projekt, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Haas-Hamann, R., Palettenchaos adé?, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Henrik, H., Blockchain ist kein Pug'n'Play, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Hermes Team, Transparenz in der Supply Chain, in: <https://newsroom.hermesworld.com> (abgerufen am 10.09.2018)

Hosp, J., Kryptowährungen: Bitcoin, Ethereum, Blockchain, ICOs & Co. Einfach erklärt, München 2018

Hyperledger, Hyperledger Fabric Explainer, in: www.youtube.com (abgerufen am 26.09.2018)

IBM, Hyperledger, in: www.ibm.com (abgerufen am 21.09.2018)

IBM, Maersk und IBM bilden Joint Venture für Blockchain, in: www.ibm.com (abgerufen am 26.09.2018)

IBMBlockchain, IBM and Maersk demo: Cross-border supply chain solution on blockchain, in: www.youtube.com, (abgerufen am 26.09.2018)

Kienzler, R., Hyperledger – eine offene Blockchain Technologie, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology: Einführung für Business- und IT Manager, Berlin/Boston 2016

Kress, W., Maersk und IBM kündigen Supply-Chain-Lösung auf Blockchain-Technologie an, in: www.ibm.com (abgerufen am 26.09.2018)

Merz, M., Einsatzpotenziale der Blockchain im Energiehandel, in: Daniel Burgwinkel (Hrsg.) Blockchain Technology: Einführung für Business- und IT Manager, Berlin/Boston 2016

Metzger, J., Konsensmechanismus, in: <https://wirtschaftslexikon.gabler.de> (abgerufen am 26.09.2018)

Mohr, O., User Centered Design: Die Palettentausch-App wird getestet, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Moneycab, IBM und Maersk führen Blockchain-Lösung TradeLens für Lieferkette ein, in: www.moneycab.com (abgerufen am 26.09.2018)

Ostler, U., Tradelens von Maersk und IBM soll das Schifffahrtsökosystem umkempeln (sic), in: www.datacenter-insider.de (abgerufen am 26.09.2018)

Ploom, M., Blockchain Business Modelle in der Finanzindustrie, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology: Einführung für Business- und IT Manager, Berlin/Boston 2016

Ploom, T., Blockchains - wichtige Fragen aus IT-Sicht, in: Daniel Burgwinkel (Hrsg.): Blockchain Technology: Einführung für Business- und IT Manager, Berlin/Boston 2016

Popper, N., How China Took Center Stage in Bitcoin's Civil War, in: www.nytimes.com (abgerufen am 25.09.2018)

Radermacher, M., Internet of Things und Blockchain in der Logistik, in: www.mm-logistik.vogel.de (abgerufen am 24.09.2018)

Rosenberger, P., Bitcoin und Blockchain: Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, Berlin 2018

Sixt, E., Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie, Wiesbaden 2017

Specht, P., Die 50 wichtigsten Themen der Digitalisierung: Künstliche Intelligenz, Blockchain, Bitcoin, Virtual Reality und vieles mehr verständlich erklärt, München 2018

Stettiner, E., Projektteam blickt auf Nutzer, in: www.gs1-germany.de (abgerufen am 26.09.2018)

The Linux Foundation, Hyperledger Fabric, in: www.hyperledger.org (abgerufen am 12.09.2018)

Tröger, R., Was haben (GS1) Standards mit Blockchain zu tun?, in: www.gs1-germany.de (abgerufen am: 26.09.2018)

Uhde, T., Das Palettenchaos auf die Kette kriegen: Die Systemarchitektur zum Pilotprojekt, in: www.gs1-germany.de (abgerufen am 26.09.2018)

Wunsch, A., Der Praxistest – Wir gehen auf Ganze!, in: www.gs1-germany.de (abgerufen am: 26.09.2018)

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne unerlaubte Hilfe angefertigt, andere als die angegebenen Quellen nicht benutzt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Winsen (Luhe), den 30.09.2018

Torben Steffen